

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-244926

(43)Date of publication of application : 30.08.2002

(51)Int.Cl.

G06F 12/14
G06F 17/60
H04L 9/08
H04N 5/765
H04N 5/781
H04N 5/85
H04N 5/91

(21)Application number : 2001-039140

(71)Applicant : MATSUSHITA ELECTRIC IND CO
LTD

(22)Date of filing : 15.02.2001

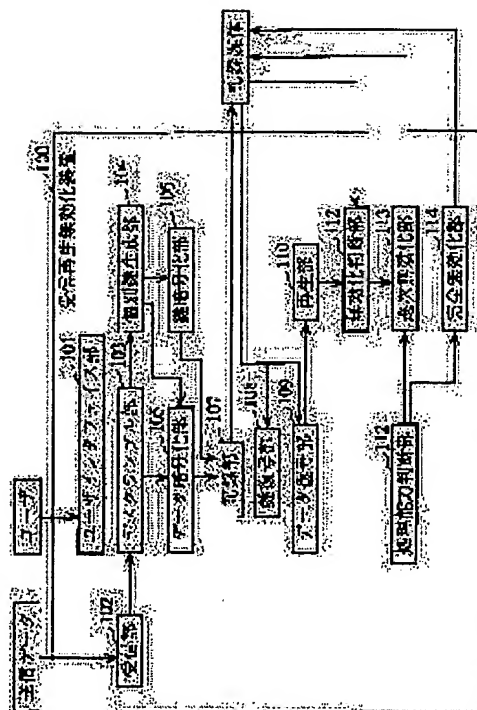
(72)Inventor : MURASE KAORU
MOTOHASHI YOSHIHIKO
MIYAZAKI MASAYA

(54) DATA INVALIDATING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data invalidating device capable of improving user's convenience without deviating from the purpose allowing no duplicate of data.

SOLUTION: This data invalidating device is provided with a receiving part 102 for receiving the data indicating that copying is not permitted, a recording part 107 dividing the received data into partial data and recording it, a reproducing part 110 for reproducing the recorded partial data sequentially, an invalidation judging part 111 judging that the partial data must be invalidated due to the expiration of recording term and the reproduction of the partial data, and a one after another invalidating part 113 for destroying at least the data required previously to utilize other data among the partial data to be invalidated one after another by substituting new data and arbitrary data.



(11)特許出願公開番号

特開2002-244926

(P2002-244926A)

(43)公開日 平成14年8月30日(2002.8.30)

(51)Int.Cl.'	識別記号	F I	テマコード(参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 D 5 B 0 1 7
			3 2 0 E 5 C 0 5 2
17/60	1 4 2	17/60	1 4 2 5 C 0 5 3
H 0 4 L 9/08		H 0 4 N 5/85	Z 5 J 1 0 4
H 0 4 N 5/765		H 0 4 L 9/00	6 0 1 C
審査請求 未請求 請求項の数39 O L (全 24 頁) 最終頁に続く			

(21)出願番号 特願2001-39140(P2001-39140)

(22)出願日 平成13年2月15日(2001.2.15)

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 村瀬 薫

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 本橋 良彦

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 100090446

弁理士 中島 司朗

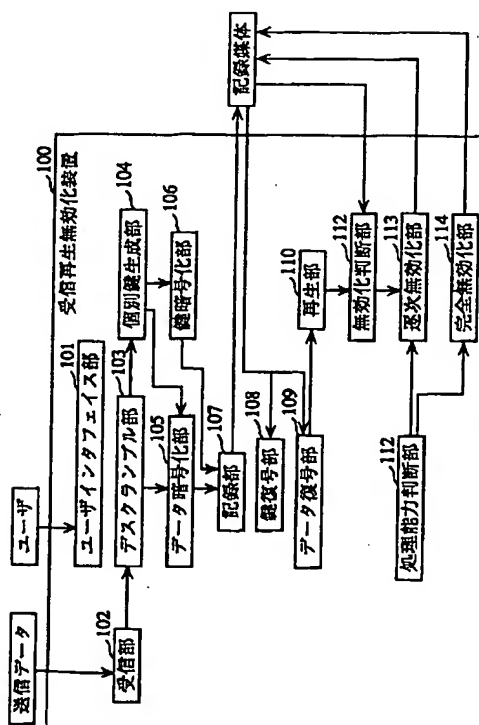
[最終頁に続く](#)

(54) 【発明の名称】 データ無効化装置

(57) 【要約】

【課題】データの複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができるデータ無効化装置を提供する。

【解決手段】コピー不可を示すデータを受信する受信部１０２と、受信されたデータを部分データに分けて記録する記録部１０７と、記録された部分データを順次再生する再生部１１０と、記録期限が切れた事や再生された事等をもって部分データを無効化すべきと判断する無効化判断部１１１と、無効化すべき部分データのうち少なくとも他のデータを利用するために先に必要となるデータを、新しいデータや任意のデータを上書きする等して逐次破壊する逐次無効化部１１３とを備える。



【特許請求の範囲】

【請求項 1】 一の記録媒体に記録された対象データを無効化するデータ無効化装置であって、

前記対象データは、複数の部分データから構成され、前記部分データ単位で前記一の記録媒体に記録された対象データを、無効化すべきか否か判断する判断手段と、前記判断手段により所定数又は所定量の部分データに対して無効化すべきと判断される度に、前記一の記録媒体に記録された対象データのうちの、当該無効化すべきと判断された部分データを逐次無効化する逐次無効化手段とを備えることを特徴とするデータ無効化装置。

【請求項 2】 前記一の記録媒体は、記録された各部分データの記録順序を示す順序情報を記録しており、前記判断手段は、前記順序情報により示される記録順序に基づいて、先に記録された部分データから順番に無効化すべきと判断することを特徴とする請求項 1 に記載のデータ無効化装置。

【請求項 3】 前記一の記録媒体に記録されている対象データは、他の装置から連続的に送信される送信データが、現在の方まで継続的に記録されているものであり、前記データ無効化装置は、さらに、前記送信データを受信する受信手段を備え、前記逐次無効化手段は、受信手段により受信された送信データを新たな部分データとし、前記一の記録媒体内の前記判断手段により無効化すべきと判断された部分データが記録されている記録領域に、前記新たな部分データを上書きすることにより、当該新しい部分データを記録しつつ当該無効化すべきと判断された部分データを無効化することを特徴とする請求項 2 に記載のデータ無効化装置。

【請求項 4】 前記部分データはそれぞれ、前記送信データの一定の送信時間分のデータであり、前記一の記録媒体には、前記一定の送信時間分のデータを記録するための記録領域が規定数だけ確保されることを特徴とする請求項 3 に記載のデータ無効化装置。

【請求項 5】 前記一定の送信時間分のデータが、常に一定のデータ量でない場合において、前記逐次無効化手段は、前記無効化すべきと判断された部分データのうちの、前記新たな部分データを上書きするだけでは全て上書きできない部分に、さらに、任意のデータを上書きすることを特徴とする請求項 4 に記載のデータ無効化装置。

【請求項 6】 前記逐次無効化手段は、前記新たな部分データの上書きを止めた後も、先に記録されている部分データを全て無効化するまでは、任意のデータを継続的に上書きすることを特徴とする請求項 4 及び 5 の何れか 1 項に記載のデータ無効化装置。

【請求項 7】 前記一の記録媒体には、記録された各部分データの記録期限を管理するための期限管理情報が記録されており、

前記判断手段は、前記期限管理情報に基づいて、記録期限が切れた部分データを無効化すべきと判断することを特徴とする請求項 1 に記載のデータ無効化装置。

【請求項 8】 前記データ無効化装置は、さらに、前記一の記録媒体に記録された対象データを、前記部分データ単位で利用する利用手段を備え、前記判断手段は、さらに、前記利用手段により利用された部分データを無効化すべきと判断することを特徴とする請求項 2 及び 7 の何れか 1 項に記載のデータ無効化装置。

【請求項 9】 前記データ無効化装置は、さらに、前記一の記録媒体に記録された対象データを、前記部分データ単位で利用する利用手段を備え、前記判断手段は、前記利用手段により利用された部分データを無効化すべきと判断することを特徴とする請求項 1 に記載のデータ無効化装置。

【請求項 10】 前記一の記録媒体に記録されている対象データは、他の装置から送信されたコンテンツデータが記録されているものであり、

前記送信されたコンテンツデータには、前記対象データのコピーの可否を示すコピー制御情報が添付されており、

前記利用手段は、前記一の記録媒体に記録されたコンテンツデータを、前記部分データ単位で再生するものであり、

前記判断手段は、前記送信されたコンテンツデータに添付されていたコピー制御情報がコピー不可を示していた場合に限り、前記利用手段により再生された部分データに対応する、前記一の記録媒体に記録された部分データを無効化すべきと判断することを特徴とする請求項 8 及び 9 の何れか 1 項に記載のデータ無効化装置。

【請求項 11】 前記一の記録媒体に記録されている対象データには、前記対象データのコピーの可否を示すコピー制御情報が添付されており、

前記利用手段は、前記一の記録媒体に記録された対象データを、前記部分データ単位で、二の記録媒体に記録するものであり、

前記判断手段は、前記コピー制御情報がコピー不可を示している場合に限り、前記利用手段により前記二の記録媒体に記録された部分データに対応する、前記一の記録媒体に記録された部分データを無効化すべきと判断することを特徴とする請求項 9 に記載のデータ無効化装置。

【請求項 12】 前記逐次無効化手段は、前記一の記録媒体上の、前記判断手段により無効化すべきと判断された部分データを全て逐次破壊することを特徴とする請求項 1 ～ 11 の何れか 1 項に記載のデータ無効化装置。

【請求項 13】 前記逐次無効化手段は、前記一の記録媒体上の、前記判断手段により無効化すべ

10

20

30

40

50

きと判断された部分データのうちの、部分データを利用する際に、他のデータを利用するために先に必要となるデータを、少なくとも逐次破壊することを特徴とする請求項 1、2 及び 7～11 の何れか 1 項に記載のデータ無効化装置。

【請求項 14】 前記一の記録媒体に記録されている対象データは、I ピクチャーを含む MPEG データであり、

前記先に必要となるデータは、I ピクチャーであることを特徴とする請求項 13 に記載のデータ無効化装置。

【請求項 15】 前記一の記録媒体に記録されている対象データは、I ピクチャーを含む MPEG データであり、

前記先に必要となるデータは、I ピクチャーの先頭のセクタであることを特徴とする請求項 13 に記載のデータ無効化装置。

【請求項 16】 前記逐次無効化手段は、自身の処理能力に余裕が無い場合には、前記少なくとも逐次破壊する部分のデータのみを逐次破壊することを特徴とする請求項 13～15 の何れか 1 項に記載のデータ無効化装置。

【請求項 17】 前記逐次無効化手段は、自身の処理能力の余裕の範囲で、前記少なくとも破壊する部分以外のデータを破壊することを特徴とする請求項 16 に記載のデータ無効化装置。

【請求項 18】 前記データ無効化装置は、さらに、前記無効化すべきと判断された部分データのうちの、前記逐次無効化手段により逐次破壊されなかった部分のデータを、前記処理能力に余裕がある時に全て破壊する完全無効化手段を備えることを特徴とする請求項 16 及び 17 の何れか 1 項に記載のデータ無効化装置。

【請求項 19】 前記一の記録媒体に記録されている対象データは、前記部分データ毎に個別の部分データ暗号鍵を用いて暗号化されており、前記一の記録媒体には、暗号化され記録された各部分データを復号するための各部分データ復号鍵が記録されており、前記逐次無効化手段は、前記一の記録媒体上の、前記判断手段により無効化すべきと判断された部分データに対応する部分データ復号鍵を、少なくとも逐次破壊することを特徴とする請求項 1、2 及び 7～11 の何れか 1 項に記載のデータ無効化装置。

【請求項 20】 前記データ無効化装置は、さらに、暗号化された前記対象データを入手する入手手段と、入手手段により入手された暗号化された対象データを、正当な使用者に予め配布された使用者鍵を用いて復号し、対象データを生成する復号手段と、前記部分データ毎に、任意の部分データ暗号鍵と、対応する部分データ復号鍵とを生成する鍵生成手段と、

復号手段により復号された対象データを、前記部分データ毎に、鍵生成手段により生成された部分データ暗号鍵を用いて、対応する部分データ復号鍵によって復号可能に暗号化するデータ暗号化手段と、

鍵生成手段により生成された部分データ復号鍵を、当該データ無効化装置に固有の識別子を用いて暗号化する鍵暗号化手段と、

データ暗号化手段により暗号化された部分データと、対応する鍵暗号化手段により暗号化された部分データ復号鍵とを、前記一の記録媒体に記録する記録手段とを備えることを特徴とする請求項 19 に記載のデータ無効化装置。

【請求項 21】 前記データ無効化装置は、少なくとも、前記復号手段、前記鍵生成手段、前記データ暗号化手段、及び、鍵暗号化手段を、同一の半導体チップ内に収めることを特徴とする請求項 20 に記載のデータ無効化装置。

【請求項 22】 一の記録媒体に記録された対象データを無効化するデータ無効化プログラムであって、前記対象データは、複数の部分データから構成され、コンピュータに、前記部分データ単位で前記一の記録媒体に記録された対象データを、無効化すべきか否かを判断する判断ステップと、前記判断ステップにより所定数又は所定量の部分データに対して無効化すべきと判断される度に、前記一の記録媒体に記録された対象データのうちの、当該無効化すべきと判断された部分データを逐次無効化する逐次無効化ステップとを実行させることを特徴とするデータ無効化プログラム。

【請求項 23】 前記一の記録媒体は、記録された各部分データの記録順序を示す順序情報を記録しており、前記判断ステップは、前記順序情報により示される記録順序に基づいて、先に記録された部分データから順番に無効化すべきと判断することを特徴とする請求項 22 に記載のデータ無効化プログラム。

【請求項 24】 前記一の記録媒体に記録されている対象データは、他の装置から連続的に送信される送信データが、現在の分まで継続的に記録されているものであり、

前記データ無効化プログラムは、さらに、コンピュータに、前記送信データを受信する受信ステップを実行させ、前記逐次無効化ステップは、受信ステップにより受信された送信データを新たな部分データとし、前記一の記録媒体内の前記判断ステップにより無効化すべきと判断された部分データが記録されている記録領域に、前記新たな部分データを上書きすることにより、当該新しい部分データを記録しつつ当該無効化すべきと判断された部分データを無効化することを特

10

20

30

40

50

徴とする請求項23に記載のデータ無効化プログラム。

【請求項25】 前記一の記録媒体には、記録された各部分データの記録期限を管理するための期限管理情報が記録されており、

前記判断ステップは、前記期限管理情報に基づいて、記録期限が切れた部分データを無効化すべきと判断することを特徴とする請求項22に記載のデータ無効化プログラム。

【請求項26】 前記データ無効化プログラムは、さらに、コンピュータに、

前記一の記録媒体に記録された対象データを、前記部分データ単位で利用する利用ステップを実行させ、

前記判断ステップは、さらに、前記利用ステップにより利用された部分データを無効化すべきと判断することを特徴とする請求項23及び25の何れか1項に記載のデータ無効化プログラム。

【請求項27】 前記データ無効化プログラムは、さらに、コンピュータに、

前記一の記録媒体に記録された対象データを、前記部分データ単位で利用する利用ステップを実行させ、

前記判断ステップは、前記利用ステップにより利用された部分データを無効化すべきと判断することを特徴とする請求項22に記載のデータ無効化プログラム。

【請求項28】 前記逐次無効化ステップは、前記一の記録媒体上の、前記判断ステップにより無効化すべきと判断された部分データを全て逐次破壊することを特徴とする請求項22～27の何れか1項に記載のデータ無効化プログラム。

【請求項29】 前記逐次無効化ステップは、前記一の記録媒体上の、前記判断手段により無効化すべきと判断された部分データのうちの、部分データを利用する際に、他のデータを利用するために先に必要となるデータを、少なくとも逐次破壊することを特徴とする請求項22、23及び25～27の何れか1項に記載のデータ無効化プログラム。

【請求項30】 前記一の記録媒体に記録されている対象データは、前記部分データ毎に個別の部分データ暗号鍵を用いて暗号化されており、

前記一の記録媒体には、暗号化され記録された各部分データを復号するための各部分データ復号鍵が記録されており、

前記逐次無効化ステップは、前記一の記録媒体上の、前記判断手段により無効化すべきと判断された部分データに対応する部分データ復号鍵を、少なくとも逐次破壊することを特徴とする請求項22、23及び25～27の何れか1項に記載のデータ無効化プログラム。

【請求項31】 一の記録媒体に記録された対象データ

を無効化するデータ無効化方法であって、

前記対象データは、複数の部分データから構成され、前記部分データ単位で前記一の記録媒体に記録された対象データを、無効化すべきか否か判断する判断ステップと、

前記判断ステップにより所定数又は所定量の部分データに対して無効化すべきと判断される度に、前記一の記録媒体に記録された対象データのうちの、当該無効化すべきと判断された部分データを逐次無効化する逐次無効化ステップとを備えることを特徴とするデータ無効化方法。

【請求項32】 前記一の記録媒体は、記録された各部分データの記録順序を示す順序情報を記録しており、前記判断ステップは、前記順序情報により示される記録順序に基づいて、先に記録された部分データから順番に無効化すべきと判断することを特徴とする請求項31に記載のデータ無効化方法。

【請求項33】 前記一の記録媒体に記録されている対象データは、他の装置から連続的に送信される送信データが、現在の分まで継続的に記録されているものであり、

前記データ無効化方法は、さらに、前記送信データを受信する受信ステップを備え、前記逐次無効化ステップは、

受信ステップにより受信された送信データを新たな部分データとし、前記一の記録媒体内の前記判断ステップにより無効化すべきと判断された部分データが記録されている記録領域に、前記新たな部分データを上書きすることにより、当該新しい部分データを記録しつつ当該無効化すべきと判断された部分データを無効化することを特徴とする請求項32に記載のデータ無効化方法。

【請求項34】 前記一の記録媒体には、記録された各部分データの記録期限を管理するための期限管理情報が記録されており、

前記判断ステップは、前記期限管理情報に基づいて、記録期限が切れた部分データを無効化すべきと判断することを特徴とする請求項31に記載のデータ無効化方法。

【請求項35】 前記データ無効化方法は、さらに、前記一の記録媒体に記録された対象データを、前記部分データ単位で利用する利用ステップを備え、

前記判断ステップは、さらに、前記利用ステップにより利用された部分データを無効化すべきと判断することを特徴とする請求項32及び34の何れか1項に記載のデータ無効化方法。

【請求項36】 前記データ無効化方法は、さらに、前記一の記録媒体に記録された対象データを、前記部分データ単位で利用する利用ステップを備え、前記判断ステップは、前記利用ステップにより利用された部分データを無効化すべきと判断することを特徴とする請求項31に記載のデータ無効化方法。

10

20

30

40

50

【請求項37】 前記逐次無効化ステップは、前記一の記録媒体上の、前記判断ステップにより無効化すべきと判断された部分データを全て逐次破壊することとを特徴とする請求項31～36の何れか1項に記載のデータ無効化方法。

【請求項38】 前記逐次無効化ステップは、前記一の記録媒体上の、前記判断手段により無効化すべきと判断された部分データのうちの、部分データを利用する際に、他のデータを利用するために先に必要となるデータを、少なくとも逐次破壊することとを特徴とする請求項31、32及び34～36の何れか1項に記載のデータ無効化方法。

【請求項39】 前記一の記録媒体に記録されている対象データは、前記部分データ毎に個別の部分データ暗号鍵を用いて暗号化されており、前記一の記録媒体には、暗号化され記録された各部分データを復号するための各部分データ復号鍵が記録されており、

前記逐次無効化ステップは、前記一の記録媒体上の、前記判断手段により無効化すべきと判断された部分データに対応する部分データ復号鍵を、少なくとも逐次破壊することとを特徴とする請求項31、32及び34～36の何れか1項に記載のデータ無効化方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、データの著作権を保護する為にデータを無効化する装置に関し、特に、著作権を保護しつつ、ユーザの利便性を高める技術に関する。

【0002】

【従来の技術】近年、情報のデジタル化が進んでいる。デジタル化された情報（以下「デジタルコンテンツ」と言う）は時間とともに劣化することがなく、また比較的取り扱い易いので、特に音声情報や画像情報のデジタル化が著しく進んでいる。しかしデジタルコンテンツはコピーしてもオリジナルと全く同じものができるので、著作権のある情報が無断で複製されたり、改ざんされたりといった不正行為が簡易に行なわれてしまうという欠点を持っている。

【0003】このような不正行為を防ぐために、デジタルコンテンツを暗号化して供給し、著作権料を支払う契約をしているような正当なユーザの装置のみに復号の為に復号鍵を付与する方法が考えられる（以下、暗号化されたデジタルコンテンツを「暗号化コンテンツ」と言う）。このようにすると、正当なユーザの装置以外の他の装置では暗号化コンテンツを復号できないのでデジタルコンテンツの不正な使用を防ぐことができる。

【0004】また、著作権保護の可否を示すために、デジタルコンテンツにはコピーの可否等を示すコピー制御

情報（CCI: Copy Control Information）を添付することがある。コピー制御情報は、「Copy Never」、「Copy one Generation」、「Copy No more」及び「Copy Free」の4つのステータスを示す。

【0005】「Copy Never」とは、デジタルコンテンツのコピーを全く許さないことを示す。「Copy one Generation」とは、一世代だけデジタルコンテンツのコピーを許すことを示す。コピーされた側のデジタルコンテンツのコピー制御情報は「Copy No more」となる。

【0006】「Copy No more」とは、「Copy one Generation」のデジタルコンテンツからコピーされたデジタルコンテンツに添付されるコピー制御情報であり、以前はコピーを許したが今はコピーを許さないことを示す。「Copy Free」とは、自由にデジタルコンテンツのコピーを許すことを示す。

【0007】ここでデジタルコンテンツが商用デジタル放送等によって伝送路を介して供給される場合には、コピー制御情報が「Copy Never」、「Copy one Generation」及び「Copy No more」のデジタルコンテンツは必ず暗号化コンテンツの状態では供給され伝送路上における安全が確保される。なお「Copy Free」のデジタルコンテンツは通常、暗号化されない状態で供給される。

【0008】

【発明が解決しようとする課題】コピー制御情報が「Copy Never」であるデジタルコンテンツを伝送路を介して入手して再生する場合や、コピー制御情報が「Copy one Generation」であるデジタルコンテンツを入手して記録媒体に記録することによりコピー制御情報が「Copy No more」であるデジタルコンテンツが生成される場合等に、これらのデジタルコンテンツのコピーを全く許さないものとするユーザにとって甚だ利便性が低い事態が考えられる。

【0009】伝送路を介して供給されるデジタルコンテンツがコピー不可でない場合は、デジタルコンテンツを受信側の記録媒体に記録しておいて後で視聴したり、HDD（ハードディスクドライブ）等の記録媒体に記録しながら再生することによりタイムシフト視聴が可能であるが、このデジタルコンテンツのコピーが全く許されない場合は、ユーザは視聴の途中でトイレに行ったり来客や電話等により視聴を中断してしまうと再放送でもない限り視聴を中断した部分を全く視聴できない。例えば、多くの映画は2時間程度が普通であり、4時間を超える長編物も珍しいものではなく、商用デジタル放送等では普通コマーシャルが無いこと等を考えると、コピー制御

情報が「Copy Never」であることによりコピーが全く許されないとされた映画等をユーザが全て視聴する為には、2～4時間もの間全くトイレに行く事もできず、来客も電話も許されないなどと言う甚だ利便性が低い事態となってしまう。

【0010】また、入手し記録媒体に記録したデジタルコンテンツがコピー不可とならない場合は、デジタルコンテンツを他の記録媒体に自由にコピーしたり移動したりすることができるが、このデジタルコンテンツのコピーが全く許されない場合は、ユーザは入手したデジタルコンテンツを一旦どこかの記録媒体に記録してしまうと後で移動することができない。例えば、HDD等のアクセス速度が速く使い勝手のよい固定記録媒体を汎用的に使用の方が利便性が高いので、ユーザは入手したデジタルコンテンツをとりあえず固定記録媒体に記録するのが普通であるが、固定記録媒体の記録容量は限られており、またHDD等の汎用記録媒体は絶えず使用されている等の理由からリムーバルな他の記録媒体に比べて壊れる可能性が高いので、ユーザが一旦視聴する等して長期に保存したいと判断したデジタルコンテンツは、記録容量が限られず保存の面で有利なDVD-RWやデジタルビデオ等のリムーバルな記録媒体に移動する事が望ましい。

【0011】とはいえ、ユーザにとっての利便性を向上させる為に、著作権保護要とされコピー不可とされたデジタルコンテンツを勝手にコピー不可でなくように変更することは著作権保護の観点から許される事ではない。本来、コピー制御情報が「Copy Never」のデジタルコンテンツは、著作権保護の観点から視聴は許すが複製品を禁止することを示し、コピー制御情報が「Copy one Generation」のデジタルコンテンツは、著作権保護の観点から1世代限りの複製品を許すことを示す筈である。

【0012】そこで、特定の条件の下でのコピーを許す代わりに確実に然るべきデジタルコンテンツを無効化することにより、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができるものと考え。本発明は、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができるデータ無効化装置、データ無効化方法、データ無効化プログラム、及び、データ無効化プログラムを記録するコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【0013】

【課題を解決するための手段】上記目的を達成するために、本発明に係るデータ無効化装置は、一の記録媒体に記録された対象データを無効化するデータ無効化装置であって、前記対象データは複数の部分データから構成され、前記部分データ単位で前記一の記録媒体に記録された対象データを無効化すべきか否か判断する判断手段と、前記判断手段により所定数又は所定量の部分データ

に対して無効化すべきと判断される度に前記一の記録媒体に記録された対象データのうちの当該無効化すべきと判断された部分データを逐次無効化する逐次無効化手段とを備えることを特徴とする。

【0014】これによって、対象データを所定数又は所定量の部分データ毎に、所定の条件が満たされた部分データを逐次無効化することができる。従って、対象データの一時的な使用は許すが複製品の生成を禁止したり、1世代限りの複製品を許す等の場合において、禁止された複製品の生成を一時的に許す代わりにその複製品又はオリジナルを無効化することができ、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができる。

【0015】また、逐次複製品を無効化するので、悪意ある者が動作の途中で電源を抜くなどの小細工をして複製品を残そうとしても、所定数又は所定量の部分データの複製品を残す事が精一杯となるため、この単位を適切に選ぶことによりセキュリティを高めることができる。

【0016】

【発明の実施の形態】（実施の形態1）

<概要>本発明の実施の形態1は、複製品を許さないという趣旨のデジタルコンテンツを受信した場合において、一時的に記録を許すが、再生した場合や予め定めた一定時間を経過した場合には無効化する装置であり、1回限りの視聴、又は、受信から一定時間内に限りタイムシフト視聴を可能とするものである。

【0017】<構成>図1は、本発明の実施の形態1に係る受信再生無効化システムのハードウェア構成の一例を示す図である。ここで図1には、説明の為に、アンテナ901、受信装置902、モニタ903、RAM904、HDD905、DVDレコーダ906及びROM907を記載している。ここで、システムLSI800、RAM904、HDD905及びROM907は通常、STB（Set Top Box）と呼ばれる同一筐体内に収納されている。

【0018】図1に示すシステムLSI800は、トランスポートストリームデコーダ801、AVデコーダ802、暗号エンジン803及びマイコン804からなり、これらを同一の半導体チップ内に収めることにより、トランスポートストリームをデコードした直後の何の暗号化もされていないデジタルデータを回路基盤の配線線に出さないようにしてセキュリティの強化を図っている。

【0019】受信装置902は、アンテナ901を介して放送局から所望の搬送波を受信して復調し、利用すべきデジタルコンテンツや制御データのペケットからなるトランスポートストリーム（以下「TSストリーム」という）を生成する。ここでは、利用すべきデジタルコンテンツが著作権保護要の場合には、例えばデジタルコン

テンツに添付されたコピー制御情報が「Copy Never」とされることなどによって複製品を許さないという趣旨の情報がデジタルコンテンツに添付され、さらにTSストリームのうち、制御情報等であるヘッダ部はそのままであるが、送信すべきデータであるペイロード部がスクランブルと呼ばれる暗号方式により暗号化される。

【0020】トランスポートストリームデコーダ801は、受信装置902により生成されたTSストリームの、スクランブルされているものに対しては予め正当なユーザに与えられる復号鍵を用いて復号（デスクランブル）してデコードし、スクランブルされていないものに対してはそのままデコードし、利用すべきデジタルコンテンツを生成する。例えばここで生成される利用すべきデジタルコンテンツは、音声及び画像のMPEGストリームである。

【0021】AVデコーダ802は、トランスポートストリームデコーダ801により生成されたデジタルコンテンツから映像出力信号及び音声出力信号を生成しモニター903に映像及び音声を再生させる。暗号エンジン803は、利用すべきデジタルコンテンツが著作権保護要の場合であって、RAM904、HDD905及びDVDレコーダ906等の記録媒体に記録が必要な場合に、トランスポートストリームデコーダ801により生成された利用すべきデジタルコンテンツを、所定の再生時間に相当する分毎に、ここでランダムに生成した暗号鍵を用いて暗号化し、対応する復号鍵をデバイスIDを用いて暗号化してセットで記録し、デジタルコンテンツを使用する際には、暗号化された復号鍵をデバイスIDを用いて復号し、これを用いて暗号化されたデジタルコンテンツを復号する。ここでデバイスIDとは、半導体チップ毎に固有の値であり、ここでは半導体チップの外部からは参照できないものとする。

【0022】マイコン804は、ROM907に記録された制御プログラムを読み出して実行することにより、STD全体の動作を制御する。ここでは制御プログラムが悪意のあるユーザに勝手に書き換えられないようにスクランブルされているものとし、デスクランブルしてから実行されるものとする。ここでユーザが、複製品を許さないという趣旨の情報が添付されたデジタルコンテンツを視聴している途中で、なんらかの所用の為にタイムシフト視聴を指示したとすると、マイコン804は暗号化させたデジタルコンテンツをHDD905に記録させ続けながら、シフト時間の分だけ前の、HDD905に記録された暗号化されたデジタルコンテンツを復号させて再生させ続けると同時に、再生されたデジタルコンテンツに対応するHDD905内の暗号化されたデジタルコンテンツを、所定の再生時間の分毎に、再生できないように順次無効化する。

【0023】ここでは、暗号化されたデジタルコンテンツ

を再生されたことを条件に無効化した。が、単に、又は、さらに、記録してから所定の時間が経過したことを条件に無効化してもよい。多くの映画は2時間程度が普通なので、この所定の時間を例えば90分程度に設定しておけば、多くの映画が記録媒体に丸々記録された状態に一瞬たりともなり得ず、処理の途中で電源を切る等しても映画の1本分も残せない。よって、後々映画の1本分を再生することはできないことになり、この所定の時間の分だけに限りタイムシフト視聴を許すことができる。

【0024】図2は、本発明の実施の形態1に係る受信再生無効化装置の機能ブロック図である。図2に示す受信再生無効化装置100は、ユーザインタフェース部101、受信部102、デスクランブル部103、個別鍵生成部104、データ暗号化部105、鍵暗号化部106、記録部107、鍵復号部108、データ復号部109、再生部110、無効化判断部111、処理能力判断部112、逐次無効化部113、完全無効化部114を備える。ここで実際には、受信部102の機能は図1の受信装置902の機能に相当し、デスクランブル部103の機能は図1のトランスポートストリームデコーダ801の機能に相当し、個別鍵生成部104、データ暗号化部105、鍵暗号化部106、記録部107、鍵復号部108、データ復号部109の機能は図1の暗号エンジン803の機能に相当し、再生部110の機能は図1のAVデコーダ802の機能に相当し、無効化判断部111、処理能力判断部112、逐次無効化部113、完全無効化部114の機能は図1のマイコン804の機能に相当する。

【0025】なお、説明を容易にするために発明と直接関係ない機能の説明は省略しているので、実際のものとは多少異なる。ユーザインタフェース部101は、ユーザから視聴指示、一時停止指示、タイムシフト視聴指示、停止指示、及び、デジタルコンテンツの移動指示等の各種の指示を受け付ける。

【0026】受信部102は、放送局等から放送される送信データを受信する。ここでは、コピー制御情報が添付されスクランブルされたデジタルコンテンツを受信するものとする。デスクランブル部103は、受信部102により受信されたスクランブルされたデジタルコンテンツを、予め正当なユーザに与えられる復号鍵を用いてデスクランブルする。

【0027】個別鍵生成部104は、ユーザが一時停止指示をしている間に、所定の放送時間に相当するデジタルコンテンツ毎に、乱数等を用いて任意の暗号鍵とこれに対応する復号鍵との組をランダムに生成する。ここでは、復号鍵と暗号鍵とが同一となるようなアルゴリズムを用いることとし、以下、復号鍵及び暗号鍵を共に生成鍵と呼ぶ。例えば10分の放送時間に相当するデジタルコンテンツ毎に、対応する生成鍵をランダムに生成す

る。

【0028】データ暗号化部105は、ユーザが一時停止指示をしている間に、デスクランブル部103によりデスクランブルされたデジタルコンテンツを、所定の放送時間に相当する分毎に、個別鍵生成部104により生成された暗号鍵を用いて、対応する復号鍵によって復号可能なように暗号化する。ここでは、10分の放送時間に相当するデジタルコンテンツを対応する生成鍵を用いて暗号化する。

【0029】鍵暗号化部106は、データ暗号化部105により暗号化に用いられた暗号鍵に対応する復号鍵を、デバイスIDを用いて暗号化する。ここでは、デバイスIDを用いて対応する生成鍵を暗号化する。記録部107は、データ暗号化部105により暗号化された所定の放送時間に相当するデジタルコンテンツと鍵暗号化部106により暗号化された対応する復号鍵との組を順次所定の記録媒体に記録する。ここでは、生成鍵を用いて暗号化された10分の放送時間に相当するデジタルコンテンツと暗号化された当該生成鍵との組を順次HDDに記録する。なお、デジタルコンテンツは、著作権保護不要の場合には暗号化せずに記録してもよい。

【0030】鍵復号部108は、ユーザがタイムシフト視聴指示をしている間に、再生すべきデジタルコンテンツに対応する暗号化された復号鍵を、先に記録された記録媒体から読み出してデバイスIDを用いて復号する。ここでは、シフト時間の分だけ前のデジタルコンテンツと組になっている暗号化された生成鍵を復号する。データ復号部109は、ユーザがタイムシフト視聴指示をしている間に、鍵復号部108により復号された復号鍵を用いて、再生すべきデジタルコンテンツを復号する。ここでは、復号された生成鍵を用いて、シフト時間の分だけ前のデジタルコンテンツを復号する。

【0031】再生部110は、ユーザが視聴指示をしている間はデスクランブル部103によりデスクランブルされたデジタルコンテンツを再生し、ユーザがタイムシフト視聴指示をしている間は、データ復号部109により復号されたデジタルコンテンツを再生する。無効化判断部111は、複製品の生成を禁止されたデジタルコンテンツであるのかかわらず受信されて一時記録された組を対象として、所定の放送時間に相当する単位で、先に記録媒体に記録された組を、所定の条件に基づいて無効化すべきか否かを判断する。ここでは、10分の放送時間に相当する暗号化されたデジタルコンテンツと暗号化された生成鍵との組単位で、無効化すべきか否かを判断する。

【0032】ここで、無効化判断部111による無効化すべき判断の条件は、再生部110により再生された事や、受信部102により受信されてから又は記録部107により記録されてから所定時間が経過した事である。なお、所定時間が経過した事をもって無効化すべきと判

断する場合には、記録部107はさらに、記録期限を管理するために所定の放送時間に相当するデジタルコンテンツの受信時刻や記録時刻等の期限管理情報を記録し、無効化判断部111はこの期限管理情報に基づいて記録期限が切れたか否かを判断する。

【0033】処理能力判断部112は、無効化すべきと判断されたデジタルコンテンツに関わるデータを全て逐次破壊するだけの処理能力の余裕が有るか否かを判断する。逐次無効化部113は、所定数又は所定量のデジタルコンテンツと復号鍵とが無効化すべきと判断される度に、先に記録されたうちの無効化すべきと判断された部分を逐次無効化する。

【0034】ここで逐次無効化部113による無効化とは、記録媒体上のデータを使用不能にすることを意味する。一般のデータ消去は、データファイルのリンク情報のみを消去したりデータファイルのヘッダ部分の数ビットのみを書き換えるだけで、データ部分がそっくりそのまま残っているのが普通であり、消去指示後にデータを復帰できる場合もあるので、このようなデータ消去ではデータを使用不能にしたとは言えない。従って、逐次無効化部113は記録媒体上の無効化すべきデータが記録されている記録領域に任意のデータを上書きしたり、その記録領域を初期化するなどしてデータそのものを破壊する。

【0035】ここで、逐次無効化部113は無効化すべきデータの全てを逐次破壊してもよいのだが、実際には、無効化すべきデータと同じサイズの任意のデータを逐次上書きすると装置自体の処理能力が問題となる場合がある。例えばタイムシフト視聴を実行している時は、放送されるデジタルコンテンツを受信し、デスクランブルし、暗号化し、記録するといった一連の処理と、記録されたデジタルコンテンツを読み出し、復号し、再生するといった一連の処理を同時にこなす必要があり、制御系及び記録媒体等の負荷が大きい。このようにただでさえ負荷の大きな処理であるところに、さらに、無効化すべきデータの全てと同じサイズの任意のデータを逐次上書きするといった負荷の大きな処理を同時に実行すると、装置自体の処理能力を高くするか、他の機能を制限することになる。

【0036】しかし、データを無効化すること自体がユーザに何の利益を与えるものでもないので、処理能力を高くすることでコストアップしたり、他の機能が制限されるような事態は避けたい。そこで逐次無効化部113は、少なくとも重要な部分を逐次破壊することとする。ここで重要な部分とは、例えば再生する際に他のデータを再生するために先に必要となるデータであり、具体的には復号鍵であり、MPEGデータにおけるIピクチャーであり、Iピクチャーの先頭のセクタである。

【0037】また、逐次無効化部113は、処理能力判断部112により処理能力の余裕があると判断された場

合に無効化すべきデータを全て破壊し、処理能力の余裕がないと判断された場合に先に必要となるデータのみを破壊することとしてもよい。完全無効化部 114 は、無効化すべきデータのうち、逐次無効化部 113 により逐次破壊されなかった部分のデータを、処理能力に余裕がある時に全て破壊する。また、ユーザがタイムシフト視聴を止める指示をした場合には、破壊されずに残っているデータを全て破壊する。

【0038】<動作 1>図 3 は、本発明の実施の形態 1 に係る受信再生無効化装置の動作の一例を示す図である。以下に図 3 を用いて、本発明の逐次再生、蓄積、タイムシフト、及び、無効化の動作を説明する。

【0039】(1) 停止状態において、ユーザインタフェイス部 101 が何らかの番組の視聴指示をユーザから受け付けるまで待つ (ステップ S1)。

(2) 視聴指示を受け付けると (ステップ S1: Yes) 逐次再生動作を開始する (ステップ S2)。受信部 102 が、ユーザにより視聴指示された番組の送信データの受信を開始する。ここでは、コピー制御情報「Copy Never」が添付されスクランブルされたデジタルコンテンツの受信を開始するものとする。

【0040】デスクランブル部 103 が、受信部 102 により受信が開始されたスクランブルされたデジタルコンテンツのデスクランブルを開始する。再生部 110 が、デスクランブル部 103 によりデスクランブルされたデジタルコンテンツの逐次再生を開始する。

(3) 逐次再生動作中において、ユーザインタフェイス部 101 が停止指示をユーザから受け付けるまで待つ (ステップ S3)。

【0041】(4) 停止指示を受け付けると (ステップ S3: Yes)、受信部 102、デスクランブル部 103、再生部 110 の各処理を停止して逐次再生動作を終了し停止状態に戻る (ステップ S4)。

(5) 逐次再生動作中において、ユーザインタフェイス部 101 が一時停止指示をユーザから受け付けるまで待つ (ステップ S5)。

【0042】(6) 一時停止指示を受け付けると (ステップ S5: Yes)、蓄積動作を開始する (ステップ S6)。

個別鍵生成部 104 が、所定の放送時間に相当するデジタルコンテンツ毎に、乱数等を用いて任意の暗号鍵とこれに対応する復号鍵との組をランダムに生成する。ここでは、10 分の放送時間に相当するデジタルコンテンツ毎に、生成鍵をランダムに生成する。

【0043】データ暗号化部 105 が、デスクランブル部 103 によりデスクランブルされたデジタルコンテンツを、所定の放送時間に相当する分毎に、個別鍵生成部 104 により生成された暗号鍵を用いて、対応する復号鍵によって復号可能なように暗号化する。ここでは、10 分の放送時間に相当するデジタルコンテンツを対応す

る生成鍵を用いて暗号化する。

【0044】鍵暗号化部 106 が、データ暗号化部 105 により暗号化に用いられた暗号鍵に対応する復号鍵を、デバイス ID を用いて暗号化する。ここでは、デバイス ID を用いて対応する生成鍵を暗号化する。記録部 107 が、データ暗号化部 105 により暗号化された所定の放送時間に相当するデジタルコンテンツと、鍵暗号化部 106 により暗号化された対応する復号鍵とを記録媒体に記録する。ここでは、生成鍵を用いて暗号化された 10 分の放送時間に相当するデジタルコンテンツと暗号化された当該生成鍵との組を HDD に記録する。

【0045】再生部 110 によるデジタルコンテンツの逐次再生を止める。

(7) 蓄積動作中において、無効化判断部 111 が、所定の放送時間に相当する単位で、先に記録媒体に記録された暗号化されたデジタルコンテンツと暗号化された復号鍵との組の中で記録期限が切れた組があるか否かを判断する。ここでは、記録期限を記録から 90 分とし、10 分の放送時間に相当する単位で、記録してから 90 分を経過した組を記録期限が切れた組と判断する (ステップ S7)。

【0046】(8) 記録期限が切れた組がある場合には、逐次無効化部 113 がその都度、記録期限が切れた組中の暗号化された復号鍵が記録された記録領域に任意のデータを上書きして、当該記録領域のデータを逐次無効化する。ここで、処理能力判断部 112 が、処理能力の余裕があると判断した場合には、さらに、記録期限が切れた組中の暗号化されたデジタルコンテンツに任意のデータを上書きして、当該記録領域のデータを逐次無効化する (ステップ S8)。

【0047】(9) 蓄積動作中において、ユーザインタフェイス部 101 が停止指示をユーザから受け付けるまで待つ (ステップ S9)。

(10) 停止指示を受け付けると (ステップ S9: Yes)、受信部 102、デスクランブル部 103、個別鍵生成部 104、データ暗号化部 105、鍵暗号化部 106、記録部 107 の各処理を停止して蓄積動作を終了し、完全無効化部 114 が、破壊されずに残っているデータを全て破壊して停止状態に戻る (ステップ S10)。

【0048】(11) 蓄積動作中において、ユーザインタフェイス部 101 がタイムシフト視聴指示をユーザから受け付けるまで待つ (ステップ S11)。

(12) タイムシフト視聴指示を受け付けると (ステップ S11: Yes)、タイムシフト動作を開始する (ステップ S12)。

鍵復号部 108 が、先に記録された記録媒体から、シフト時間の分だけ前のデジタルコンテンツと組になっている暗号化された復号鍵を読み出して、デバイス ID を用いて復号する。ここでは、シフト時間を 30 分とし、3

0分～20分前の10分間に相当するデジタルコンテンツと組になっている暗号化された生成鍵から復号を開始する。なお、シフト時間が記録期限を越える場合には、シフト時間の分だけ前の組は既に無効化されているので再生できないため、この場合のシフト時間を記録期限として動作を続行する。

【0049】データ復号部109が、鍵復号部108により復号された復号鍵を用いて、対応するデジタルコンテンツの復号を開始する。ここでは、復号された生成鍵を用いて、30分～20分前の10分間に相当するデジタルコンテンツから復号を開始する。再生部110が、データ復号部109により復号されたデジタルコンテンツの再生を開始する。

【0050】(13) タイムシフト動作中において、無効化判断部111が、所定の放送時間に相当する単位で、先に記録媒体に記録された暗号化されたデジタルコンテンツと暗号化された復号鍵との組の中で記録期限が切れたか、又は、再生部110により再生されたデジタルコンテンツに対応する組が有るか否かを判断する。ここでは、記録期限を90分とし、10分の放送時間に相当する単位で、記録してから90分を経過した、又は、再生されたデジタルコンテンツを無効化すべき組と判断する(ステップS13)。

【0051】(14) 無効化すべき組がある場合には、逐次無効化部113がその都度、無効化すべき組中の暗号化された復号鍵が記録された記録領域に任意のデータを上書きして、当該記録領域のデータを逐次無効化する。ここで、処理能力判断部112が、処理能力の余裕が有ると判断した場合には、さらに、無効化すべき組中の暗号化されたデジタルコンテンツに任意のデータを上書きして、当該記録領域のデータを逐次無効化する(ステップS14)。

【0052】(15) タイムシフト動作中において、ユーザインタフェース部101が停止指示をユーザから受け付けるまで待つ(ステップS15)。

(16) 停止指示を受け付けると(ステップS15: Yes)、受信部102、デスクランブル部103、個別鍵生成部104、データ暗号化部105、鍵暗号化部106、記録部107、鍵復号部108、データ復号部109、再生部110の各処理を停止してタイムシフト動作を終了し、完全無効化部114が、破壊されずに残っているデータを全て破壊して停止状態に戻る(ステップS16)。

【0053】(17) タイムシフト動作中において、ユーザインタフェース部101が一時停止指示をユーザから受け付けるまで待つ(ステップS17)。

(18) 一時停止指示を受け付けると(ステップS17: Yes)、鍵復号部108、データ復号部109、再生部110の各処理を停止して蓄積動作に移行する(ステップS18)。

【0054】<動作2>動作1では、逐次再生動作中は蓄積動作は行わず、一時停止指示をユーザから受け付けた場合に逐次再生動作を止めて蓄積動作に移行したが、動作2では、逐次再生動作中において蓄積動作を同時に行い、ユーザが一時停止を指示していなくてもタイムシフト視聴指示を可能にし、さらに、一時停止時間が上限に達すると自動的に一時停止を解除してタイムシフト動作に移行する自動一時停止解除機能を追加するものである。

【0055】図4は、本発明の実施の形態1に係る受信再生無効化装置の動作の別の例を示す図である。なお、受信部102により受信されるデジタルコンテンツには、記録期限(Storage Time)と再視聴期限(View Time)とが添付されているものとする。ここで、記録期限とは各組毎に記録されてから記録が許されるまでの時間を、再視聴期限とは各組毎に最初に再生されてから再視聴が許されるまでの時間を示し、記録期限と再視聴期限のどちらか一方でも経過した組を無効化すべき対象とする。

【0056】以下に図4を用いて、本発明の逐次再生蓄積、蓄積、タイムシフト、無効化、及び、自動一時停止解除の動作を説明する。なお、実施の形態1と同様の動作ステップには同じ番号を付す。

(1) 停止状態において、ユーザインタフェース部101が何らかの番組の視聴指示をユーザから受け付けるまで待つ(ステップS1)。

【0057】(2) 視聴指示を受け付けると(ステップS1: Yes) 逐次再生蓄積動作を開始する(ステップS102)。

受信部102が、ユーザにより視聴指示された番組の送信データの受信を開始する。ここでは、コピー制御情報「Copy Never」が添付されスクランブルされたデジタルコンテンツの受信を開始するものとする。

【0058】デスクランブル部103が、受信部102により受信が開始されたスクランブルされたデジタルコンテンツのデスクランブルを開始する。再生部110が、デスクランブル部103によりデスクランブルされたデジタルコンテンツの逐次再生を開始する。個別鍵生成部104が、所定の放送時間に相当するデジタルコンテンツ毎に、乱数等を用いて任意の暗号鍵とこれに対応する復号鍵との組をランダムに生成する。ここでは、10分の放送時間に相当するデジタルコンテンツ毎に、生成鍵をランダムに生成する。

【0059】データ暗号化部105が、デスクランブル部103によりデスクランブルされたデジタルコンテンツを、所定の放送時間に相当する分毎に、個別鍵生成部104により生成された暗号鍵を用いて、対応する復号鍵によって復号可能なように暗号化する。ここでは、10分の放送時間に相当するデジタルコンテンツを対応する生成鍵を用いて暗号化する。

【0060】鍵暗号化部106が、データ暗号化部105により暗号化に用いられた暗号鍵に対応する復号鍵を、デバイスIDを用いて暗号化する。ここでは、デバイスIDを用いて対応する生成鍵を暗号化する。記録部107が、データ暗号化部105により暗号化された所定の放送時間に相当するデジタルコンテンツと、鍵暗号化部106により暗号化された対応する復号鍵とを記録媒体に記録する。ここでは、生成鍵を用いて暗号化された10分の放送時間に相当するデジタルコンテンツと暗号化された当該生成鍵との組をHDDに記録する。

【0061】ここで、記録媒体に記録されるそれぞれの組には期限管理情報とともに記録期限と再視聴期限とが添付され、一度再生された組には最初の再生時刻が期限管理情報に付加されるものとする。

(3) 逐次再生蓄積動作中において、無効化判断部111が期限管理情報を参照して、所定の放送時間に相当する単位で、先に記録媒体に記録された暗号化されたデジタルコンテンツと暗号化された復号鍵との組の中で、記録期限が切れた組が有るか否かを判断し、さらに、再生された組に対しては、再視聴期限が切れた組が有るか否かを判断する。ここでは、記録期限を記録から90分、再視聴期限を再生から60分とし、10分の放送時間に相当する単位で、記録してから90分を経過した組を記録期限が切れた組と判断し、さらに、視聴から60分を経過した組を再視聴期限が切れた組と判断する(ステップS103)。

【0062】(4) 記録期限又は再視聴期限が切れた組がある場合には、逐次無効化部113がその都度、記録期限又は再視聴期限が切れた組中の暗号化された復号鍵が記録された記録領域に任意のデータを上書きして、当該記録領域のデータを逐次無効化する。ここで、処理能力判断部112が、処理能力の余裕が有ると判断した場合には、さらに、記録期限又は再視聴期限が切れた組中の暗号化されたデジタルコンテンツに任意のデータを上書きして、当該記録領域のデータを逐次無効化する(ステップS104)。

【0063】(5) 逐次再生蓄積動作中において、ユーザインタフェイス部101が停止指示をユーザから受け付けるまで待つ(ステップS105)。

(6) 停止指示を受け付けると(ステップS105: Yes)、受信部102、デスクランブル部103、再生部110、個別鍵生成部104、データ暗号化部105、鍵暗号化部106、記録部107の各処理を停止して逐次再生蓄積動作を終了し、完全無効化部114が、破壊されずに残っているデータを全て破壊して停止状態に戻る(ステップS106)。

【0064】(7) 逐次再生蓄積動作中において、ユーザインタフェイス部101がタイムシフト視聴指示をユーザから受け付けるまで待つ(ステップS107)。

(8) 逐次再生蓄積動作中において、ユーザインタフェ

イス部101が一時停止指示をユーザから受け付けるまで待つ(ステップS108)。

(9) 一時停止指示を受け付けると(ステップS108: Yes)、再生動作を終了し、蓄積動作を継続する(ステップS109)。

【0065】再生部110によるデジタルコンテンツの逐次再生を止める。

(10) 蓄積動作中において、無効化判断部111が期限管理情報を参照して、所定の放送時間に相当する単位で、先に記録媒体に記録された暗号化されたデジタルコンテンツと暗号化された復号鍵との組の中で、記録期限が切れた組が有るか否かを判断し、さらに、再生された組に対しては、再視聴期限が切れた組が有るか否かを判断する(ステップS110)。

【0066】(11) 記録期限又は再視聴期限が切れた組がある場合には、逐次無効化部113がその都度、記録期限又は再視聴期限が切れた組中の暗号化された復号鍵が記録された記録領域に任意のデータを上書きして、当該記録領域のデータを逐次無効化する。ここで、処理能力判断部112が、処理能力の余裕が有ると判断した場合には、さらに、記録期限又は再視聴期限が切れた組中の暗号化されたデジタルコンテンツに任意のデータを上書きして、当該記録領域のデータを逐次無効化する(ステップS111)。

【0067】(12) 蓄積動作中において、ユーザインタフェイス部101が停止指示をユーザから受け付けるまで待つ(ステップS9)。

(13) 停止指示を受け付けると(ステップS9: Yes)、受信部102、デスクランブル部103、個別鍵生成部104、データ暗号化部105、鍵暗号化部106、記録部107の各処理を停止して蓄積動作を終了し、完全無効化部114が、破壊されずに残っているデータを全て破壊して停止状態に戻る(ステップS10)。

【0068】(14) 蓄積動作中において、ユーザインタフェイス部101がタイムシフト視聴指示をユーザから受け付けるまで待つ(ステップS11)。

(15) 蓄積動作中において、逐次無効化部113がシフト時間が上限値に達しているか否かを判断する。上限値に達している場合はシフト時間を上限値に設定して自動的に一時停止を解除してタイムシフト動作へ移行する(ステップS115)。ここでは、シフト時間の上限値を記録期限と同じ90分とし、これによって一度も再生されないまま記録期限が切れることにより無効化されるデータをなくすことができる。

【0069】(16) 自動一時停止解除の場合(ステップS115: Yes)、又は、タイムシフト視聴指示を受け付けると(ステップS107: Yes)ステップS11: Yes)、タイムシフト動作を開始する(ステップS116)。

鍵復号部108が、先に記録された記録媒体から、シフト時間の分だけ前のデジタルコンテンツと組になっている暗号化された復号鍵を読み出して、デバイスIDを用いて復号する。ここでは、シフト時間を30分とし、30分～20分前の10分間に相当するデジタルコンテンツと組になっている暗号化された生成鍵から復号を開始する。なお、シフト時間が記録期限を越える場合には、シフト時間の分だけ前の組は既に無効化されているので再生できないため、この場合のシフト時間を記録期限として動作を続行する。

【0070】データ復号部109が、鍵復号部108により復号された復号鍵を用いて、対応するデジタルコンテンツの復号を開始する。ここでは、復号された生成鍵を用いて、30分～20分前の10分間に相当するデジタルコンテンツから復号を開始する。再生部110が、データ復号部109により復号されたデジタルコンテンツの再生を開始する。

【0071】(17) タイムシフト動作中において、無効化判断部111が期限管理情報を参照して、所定の放送時間に相当する単位で、先に記録媒体に記録された暗号化されたデジタルコンテンツと暗号化された復号鍵との組の中で、記録期限が切れた組が有るか否かを判断し、さらに、再生された組に対しては、再視聴期限が切れた組が有るか否かを判断する(ステップS117)。

【0072】(18) 記録期限又は再視聴期限が切れた組がある場合には、逐次無効化部113がその都度、記録期限又は再視聴期限が切れた組中の暗号化された復号鍵が記録された記録領域に任意のデータを上書きして、当該記録領域のデータを逐次無効化する。ここで、処理能力判断部112が、処理能力の余裕の有ると判断した場合には、さらに、記録期限又は再視聴期限が切れた組中の暗号化されたデジタルコンテンツに任意のデータを上書きして、当該記録領域のデータを逐次無効化する(ステップS118)。

【0073】(19) タイムシフト動作中において、ユーザインタフェース部101が停止指示をユーザから受け付けるまで待つ(ステップS15)。

(20) 停止指示を受け付けると(ステップS15: Yes)、受信部102、デスクランブル部103、個別鍵生成部104、データ暗号化部105、鍵暗号化部106、記録部107、鍵復号部108、データ復号部109、再生部110の各処理を停止してタイムシフト動作を終了し、完全無効化部114が、破壊されずに残っているデータを全て破壊して停止状態に戻る(ステップS16)。

【0074】(21) タイムシフト動作中において、ユーザインタフェース部101が一時停止指示をユーザから受け付けるまで待つ(ステップS17)。

(22) 一時停止指示を受け付けると(ステップS17: Yes)、鍵復号部108、データ復号部109、

再生部110の各処理を停止して蓄積動作に移行する(ステップS18)。

【0075】以上のように、本発明の実施の形態1によれば、複製品の生成が禁止されたデジタルコンテンツに対して、一時記録してタイムシフト視聴を許しながらも、記録物を逐次無効化することができるので、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができる。

(実施の形態2)

10 <概要>本発明の実施の形態2は、複製品を許さないという趣旨のデジタルコンテンツを受信した場合において、一時的に記録を許すが、一定時間を経過した場合には無効化する装置であり、無効化すべきデジタルコンテンツが記録された記録領域に新しいデジタルコンテンツを順次上書きすることによって、処理能力に影響を与えずに一定時間を経過したデジタルコンテンツを無効化する装置であり、受信から一定時間内に限りタイムシフト視聴を可能とするものである。

20 【0076】<構成>本発明の実施の形態2に係る受信再生無効化装置のハードウェア構成は、実施の形態1と同様である。図5は、本発明の実施の形態2に係る受信再生無効化装置の機能ブロック図である。

30 【0077】図5に示す受信再生無効化装置200は、ユーザインタフェース部101、受信部102、デスクランブル部103、個別鍵生成部104、データ暗号化部105、鍵暗号化部106、記録部201、鍵復号部108、データ復号部109、再生部110、無効化判断部202、処理能力判断部112、逐次無効化部203、完全無効化部204を備える。ここで実際には、受信部102の機能は図1の受信装置902の機能に相当し、デスクランブル部103の機能は図1のトランスポートストリームデコーダ801の機能に相当し、個別鍵生成部104、データ暗号化部105、鍵暗号化部106、記録部201、鍵復号部108、データ復号部109の機能は図1の暗号エンジン803の機能に相当し、再生部110の機能は図1のAVデコーダ802の機能に相当し、無効化判断部202、処理能力判断部112、逐次無効化部203、完全無効化部204の機能は図1のマイコン804の機能に相当する。

40 【0078】なお、実施の形態1と同様の構成要素には同じ番号を付し、その説明を省略する。記録部201は、データ暗号化部105により暗号化された所定の放送時間に相当するデジタルコンテンツと鍵暗号化部106により暗号化された対応する復号鍵との組を順次所定の記録媒体に記録するが、複製品の生成を禁止されたデジタルコンテンツを記録する場合には、記録媒体上に、所定の放送時間に相当するデータを記録できる容量の記録領域を複数確保し、確保した記録領域に対して順番に、データ暗号化部105により暗号化された所定の放送時間に相当するデジタルコンテンツと鍵暗号化部10

6により暗号化された対応する復号鍵との組を記録する。ここでは、10分の放送時間に相当するデータを記録できる容量の記録領域をHDD上に9個確保し、9個確保した記録領域に対して順番に、生成鍵を用いて暗号化された10分の放送時間に相当するデジタルコンテンツと暗号化された当該生成鍵との組を記録する。この時、先に記録された組が有る場合には、データを上書きする。なお、デジタルコンテンツは、著作権保護不要の場合には暗号化せずに記録してもよい。

【0079】無効化判断部202は、複製品の生成を禁止されたデジタルコンテンツであるにもかかわらず受信されて一時記録された組を対象として、所定の放送時間に相当する単位で、先に記録媒体に記録された組を、所定の条件に基づいて無効化すべきか否かを判断する。ここでは、10分の放送時間に相当する暗号化されたデジタルコンテンツと暗号化された生成鍵との組単位で、無効化すべきか否かを判断する。

【0080】ここで、無効化判断部202による無効化すべき判断の条件は、再生部110により再生された事や、受信部102により受信されてから又は記録部201により記録されてから所定時間が経過した事である。ここでは、記録媒体に記録された各組の記録順序を示す順序情報を記録しておき、先に記録された組から順番に無効化すべきと判断し、記録部201が無効化すべきと判断された組が記録された記録領域に新しい組を上書きすることにより、記録媒体上に9個確保した記録領域のそれぞれに書き込まれた10分の放送時間に相当する組は、それぞれ90分後に新しい組のデータが上書きされることにより無効化される。

【0081】逐次無効化部203は、所定数又は所定量のデジタルコンテンツと復号鍵とが無効化すべきと判断される度に、先に記録されたうちの無効化すべきと判断された部分を逐次無効化する。ここでは、新しい組のデータを記録している間は、記録すると同時に逐次無効化することができ、新しい組のデータを記録しなくなった場合には、記録媒体上の無効化すべきデータが記録されている記録領域に継続的に任意のデータを上書きするなどしてデータそのものを破壊する。

【0082】ここで、記録すべきデータが、時間あたりのデータ量が一定であるような固定ビットレートである場合には、無効化すべきデータが新しいデータの上書きによって全て無効化されるが、MPEGのように可変ビットレートである場合には無効化すべきデータが新しいデータの上書きによって全て無効化されないことがある。

【0083】そこで、逐次無効化部203は新しいデータの上書きによって無効化されなかった部分に意味のないデータを上書きするなどして、無効化すべきデータの全てを逐次破壊してもよいのだが、処理能力判断部112により処理能力の余裕があると判断された場合に無効

化すべきデータを全て破壊し、処理能力の余裕がないと判断された場合には新しいデータの上書きによって無効化されなかった部分をそのままにすることとしてもよい。

【0084】完全無効化部204は、無効化すべきデータのうち、逐次無効化部203により逐次破壊されなかった部分のデータを、処理能力に余裕がある時に全て破壊する。また、ユーザがタイムシフト視聴を止める指示をした場合には、破壊されずに残っているデータを全て破壊する。

<動作>図6は、本発明の実施の形態2に係る受信再生無効化装置の動作の一例を示す図である。

【0085】以下に図6を用いて、本発明の逐次再生、蓄積、タイムシフト、及び、無効化の動作を説明する。なお、実施の形態1と同様の動作ステップには同じ番号を付し、その説明を省略する。(1)～(5)実施の形態1の図3の(1)～(5)に同じ(ステップS1～S5)。

(6)一時視聴停止指示を受け付けると(ステップS5: Yes)、蓄積動作を開始する(ステップS21)。

【0086】個別鍵生成部104が、所定の放送時間に相当するデジタルコンテンツ毎に、乱数等を用いて任意の暗号鍵とこれに対応する復号鍵との組をランダムに生成する。ここでは、10分の放送時間に相当するデジタルコンテンツ毎に、生成鍵をランダムに生成する。データ暗号化部105が、デスクランブル部103によりデスクランブルされたデジタルコンテンツを、所定の放送時間に相当する分毎に、個別鍵生成部104により生成された暗号鍵を用いて、対応する復号鍵によって復号可能のように暗号化する。ここでは、10分の放送時間に相当するデジタルコンテンツを対応する生成鍵を用いて暗号化する。

【0087】鍵暗号化部106が、データ暗号化部105により暗号化に用いられた暗号鍵に対応する復号鍵を、デバイスIDを用いて暗号化する。ここでは、デバイスIDを用いて対応する生成鍵を暗号化する。記録部201が、記録媒体上に、所定の放送時間に相当するデータを記録できる容量の記録領域を複数確保し、確保した記録領域に対して順番に、データ暗号化部105により暗号化された所定の放送時間に相当するデジタルコンテンツと鍵暗号化部106により暗号化された対応する復号鍵との組を記録する。ここでは、10分の放送時間に相当するデータを記録できる容量の記録領域をHDD上に9個確保し、9個確保した記録領域に対して順番に、生成鍵を用いて暗号化された10分の放送時間に相当するデジタルコンテンツと暗号化された当該生成鍵との組を記録する。この時、先に記録された組が有る場合には、データを上書きする。

【0088】逐次無効化部203が、新しいデータの上

書きによって無効化されなかった部分に意味のないデータを上書きするなどして、無効化すべきデータの全てを逐次破壊する。再生部110によるデジタルコンテンツの逐次再生を止める。

(7) 実施の形態1の図3の(9)に同じ(ステップS9)。

(8) 停止指示を受け付けると(ステップS9: Yes)、受信部102、デスクランブル部103、個別鍵生成部104、データ暗号化部105、鍵暗号化部106、記録部201の各処理を停止して蓄積動作を終了し、完全無効化部204が、破壊されずに残っているデータを全て破壊して停止状態に戻る(ステップS22)。

(9)～(10) 実施の形態1の図3の(11)～(12)に同じ(ステップS11～S12)。

(11) 実施の形態1の図3の(15)に同じ(ステップS15)。

(12) 停止指示を受け付けると(ステップS15: Yes)、受信部102、デスクランブル部103、個別鍵生成部104、データ暗号化部105、鍵暗号化部106、記録部201、鍵復号部108、データ復号部109、再生部110の各処理を停止してタイムシフト動作を終了し、完全無効化部204が、破壊されずに残っているデータを全て破壊して停止状態に戻る(ステップS23)。

(13)～(14) 実施の形態1の図3の(17)～(18)に同じ(ステップS17～ステップS18)。

【0089】以上のように、本発明の実施の形態2によれば、複製品の生成が禁止されたデジタルコンテンツに対して、一時記録してタイムシフト視聴を許しながらも、新しいデータを記録することで所定時間前のデータを削除し記録物を逐次無効化することができるので、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができると同時に、逐次無効化の処理を追加しているにも関わらず装置の負荷がほとんど増えない。

【0090】(実施の形態3)

<概要>本発明の実施の形態3は、複製品を一代だけ許すという趣旨のデジタルコンテンツを受信して記録媒体に記録した場合において、他の記録媒体に移動を許すが、移動元の記録媒体上にデジタルコンテンツが残らないように、少しづつコピーしては逐次無効化するものである。

【0091】<構成>本発明の実施の形態3に係る受信再生無効化装置のハードウェア構成は、実施の形態1と同様である。ただしマイコン804に、以下の機能を追加する。ユーザが複製品を一代だけ許すという趣旨の情報が添付されたデジタルコンテンツを受信してHDD905に記録した場合において、マイコン804はHDD905に記録された暗号化されたデジタルコンテンツ

を、所定の再生時間の分毎に、コピーすると同時にコピー元のHDD905内の暗号化されたデジタルコンテンツを再生できないように順次無効化する。

【0092】図7は、本発明の実施の形態3に係る受信再生無効化装置の機能ブロック図である。図7に示す受信再生無効化装置300は、ユーザインタフェース部101、受信部102、デスクランブル部103、個別鍵生成部104、データ暗号化部105、鍵暗号化部106、記録部107、鍵復号部108、データ復号部109、再生部110、移動部301、無効化判断部302、処理能力判断部112、逐次無効化部113、完全無効化部114を備える。ここで実際には、受信部102の機能は図1の受信装置902の機能に相当し、デスクランブル部103の機能は図1のトランスポートストリームデコーダ801の機能に相当し、個別鍵生成部104、データ暗号化部105、鍵暗号化部106、記録部107、鍵復号部108、データ復号部109の機能は図1の暗号エンジン803の機能に相当し、再生部110の機能は図1のAVデコーダ802の機能に相当し、移動部301、無効化判断部302、処理能力判断部112、逐次無効化部113、完全無効化部114の機能は図1のマイコン804の機能に相当する。

【0093】なお、実施の形態1と同様の構成要素には同じ番号を付し、その説明を省略する。移動部301は、先に記録媒体に記録された組を順次他の記録媒体に移動する。ここでいう移動とは、データを他の記録媒体にコピーしたのち、元の記録媒体上のデータ部分はそのまま、データの管理情報のみをデータが消去されている状態に書き換えることを指す。ここでは、HDDに記録された組を順次他の記録媒体に移動するものとする。

【0094】無効化判断部302は、複製品を一代だけ許すデジタルコンテンツであるのもかかわらず一旦記録された後で他の記録媒体に記録された組を対象として、所定の条件に基づいて無効化すべきか否かを判断する。ここでは、10分の放送時間に相当する暗号化されたデジタルコンテンツと暗号化された生成鍵との組単位で、無効化すべきか否かを判断する。

【0095】ここで、無効化判断部302による無効化すべき判断の条件は、移動部301により移動された事である。

<動作>図8は、本発明の実施の形態3に係る受信再生無効化装置の動作の一例を示す図である。

【0096】以下に図8を用いて、本発明の移動及び無効化の動作を説明する。ここでは、実施の形態1の様な動作により、コピー制御情報「Copy one Generation」が添付されスクランブルされたデジタルコンテンツが受信されて記録される事により、所定の放送時間に相当する暗号化されたデジタルコンテンツと暗号化された生成鍵との組が複数、コピー制御情報「Copy No more」が添付されてHDDに記録

されているものとする。

【0097】(1) 停止状態において、ユーザインタフェース部101が、何らかのデジタルコンテンツの移動指示をユーザから受け付けるまで待つ(ステップS31)。

(2) デジタルコンテンツの移動指示を受け付けると(ステップS31: Yes)、無効化判断部302が、移動部301により移動された組が、コピー制御情報「Copy No more」が添付されている等により、コピーを許さないことを示すデジタルコンテンツであるかを判断する(ステップS32)。

【0098】(3) コピーを許さないことを示さないデジタルコンテンツである場合は(ステップS32: No)、移動部301が、移動すべきデジタルコンテンツの全ての組を他の記録媒体に移動する(ステップS33)。

(4) コピーを許さないことを示すデジタルコンテンツである場合は(ステップS32: Yes)、移動部301が、移動すべきデジタルコンテンツの組の1つを他の記録媒体に移動する。ここでは、HDDに記録された10分の放送時間に相当する組の1つを他の記録媒体に移動する。

【0099】(5) 移動部301により移動され、まだ無効化されていない組が所定数又は所定量だけ有るかを判断する(ステップS35)。

(6) 移動され無効化されていない組が所定数又は所定量だけ有る場合は(ステップS35: Yes)、逐次無効化部113が先に記録されたうちの無効化すべきと判断された部分を逐次無効化する(ステップS36)。

【0100】(7) 移動すべきデジタルコンテンツの全ての組を移動したかを判断する(ステップS37)。

(8) 全てを移動した場合は(ステップS32: Yes)、完全無効化部114が、無効化すべきデータのうち、逐次無効化部113により逐次破壊されなかった部分のデータを全て破壊する(ステップS38)。

【0101】以上のように、本発明の実施の形態3によれば、複製品の生成が禁止されたデジタルコンテンツに対して、移動を許しながらも、移動元のデータを逐次無効化することができるので、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができる。なお、上記実施の形態1～3では、所定の放送時間に相当するデジタルコンテンツ毎に異なる暗号鍵を生成し、生成した暗号鍵を用いて所定の放送時間に相当するデジタルコンテンツをそれぞれ暗号化したが、ある程度まとまった放送時間に相当するデジタルコンテンツや連続して記録した1まとまりのデジタルコンテンツを同じ暗号鍵を用いて暗号化してもよいし、同一の記録媒体に記録されるデジタルコンテンツを記録媒体に固有の暗号鍵を用いて暗号化してもよい。

【0102】また、上記実施の形態1～3では、暗号化されたデジタルコンテンツを逐次破壊する際に対応する復号鍵のみを破壊してもよいとしたが、上述のように所定の放送時間に相当するデジタルコンテンツを暗号化する際に共通する暗号鍵を用いた場合には、共通する復号鍵を逐次破壊すると同じ復号鍵を使用する他のデジタルコンテンツを復号できなくなってしまうので、復号鍵は逐次破壊しないでデータそのものの一部又は全部を破壊するものとする。もちろん同じ復号鍵を使用するデジタルコンテンツを全て無効化した後にその復号鍵を破壊してもよい。

【0103】また、通常データはファイルとして記録され管理されるので、上記実施の形態1～3における所定の放送時間に相当するデジタルコンテンツを含む組毎に個々のファイルとして記録してもよいし、ある程度まとまった放送時間に相当するデジタルコンテンツや連続して記録した1まとまりのデジタルコンテンツを含む複数の組を同じファイルとして記録してもよい。ここで、デジタルコンテンツを無効化する際に、組毎に個々のファイルとして記録している場合にはファイル単位で無効化の処理を行えばよいが、複数の組を同じファイルとして記録している場合には、ファイルを部分的に無効化することになり、無効化された部分を誤ってアクセスしないように無効化された部分へのアクセスを制限する。例えば、通常のオペレーティングシステムに搭載されているファイルポインタのシーク制限機能を用いることによってファイルの一部分へのアクセスを制限することができる。

【0104】また、上記実施の形態3において、記録部201が記録媒体上に複数確保する各記録領域は、必ずしも連続領域でなくてもかまわない。例えば、4Mbpsの映像音声データは10分あたり300MBにもなるので、HDD上にこれだけの領域を連続領域として確保することは効率的ではない。従って、各記録領域はそれぞれ複数の細かな連続領域により構成されることになり、各記録領域と細かな連続領域との関係はファイルシステムが独立に管理し、ファイルシステムは各記録領域を上位のアプリケーションに対してそれぞれ連続した領域として提示してファイルポインタを用いたアクセスを実現するのである。

【0105】また、コンピュータに本実施の形態1～3のような動作を実行させることができるプログラムがコンピュータ読み取り可能な記録媒体に記録され、この記録媒体が流通し取り引きの対象となりうる。また、当該プログラムは、例えばネットワーク等を介して流通し、取り引きの対象となりうる。ここでコンピュータ読み取り可能な記録媒体とは、例えば、フロッピー(登録商標)ディスク、CD、MO、DVD、メモリカード等の着脱可能な記録媒体、及び、ハードディスク、半導体メモリ等の固定記録媒体等であり、特に限定されるもので

はない。

【0106】

【発明の効果】本発明に係るデータ無効化装置は、一の記録媒体に記録された対象データを無効化するデータ無効化装置であって、前記対象データは複数の部分データから構成され、前記部分データ単位で前記一の記録媒体に記録された対象データを無効化すべきか否かを判断する判断手段と、前記判断手段により所定数又は所定量の部分データに対して無効化すべきと判断される度に前記一の記録媒体に記録された対象データのうちの当該無効化すべきと判断された部分データを逐次無効化する逐次無効化手段とを備えることを特徴とする。

【0107】これによって、対象データを所定数又は所定量の部分データ毎に、所定の条件が満たされた部分データを逐次無効化することができる。従って、対象データの一時的な使用は許すが複製品の生成を禁止したり、1世代限りの複製品を許す等の場合において、禁止された複製品の生成を一時的に許す代わりにその複製品又はオリジナルを無効化することができ、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができる。

【0108】また、逐次複製品を無効化するので、悪意ある者が動作の途中で電源を抜くなどの小細工をして複製品を残そうとしても、所定数又は所定量の部分データ分の複製品を残す事が精一杯となるため、この単位を適切に選ぶことによりセキュリティを高めることができる。また、データ無効化装置において、前記一の記録媒体は記録された各部分データの記録順序を示す順序情報を記録しており、前記判断手段は前記順序情報により示される記録順序に基づいて、先に記録された部分データから順番に無効化すべきと判断することを特徴とすることもできる。

【0109】これによって、先に記録された部分データから順番に無効化すべきと判断することができる。従って、先に記録された部分データから順番に無効化するので、常に新しい部分データだけを記録しておくことができる。また、データ無効化装置において、前記一の記録媒体に記録されている対象データは他の装置から連続的に送信される送信データが現在の分まで継続的に記録されているものであり、前記データ無効化装置は、さらに、前記送信データを受信する受信手段を備え、前記逐次無効化手段は、受信手段により受信された送信データを新たな部分データとし前記一の記録媒体内の前記判断手段により無効化すべきと判断された部分データが記録されている記録領域に前記新たな部分データを上書きすることにより当該新しい部分データを記録しつつ当該無効化すべきと判断された部分データを無効化することを特徴とすることもできる。

【0110】これによって、無効化すべきと判断された部分データが記録されている記録領域に、新たな部分デ

ータを上書きすることができる。従って、新しい部分データを記録することが無効化する処理を兼ねるので、無効化する処理が追加されたにもかかわらず装置の負荷がほとんど増加しない。また、データ無効化装置において、前記部分データはそれぞれ前記送信データの一定の送信時間分のデータであり、前記一の記録媒体には前記一定の送信時間分のデータを記録するための記録領域が規定数だけ確保されることを特徴とすることもできる。

【0111】これによって、一定の送信時間分のデータを記録するための記録領域を規定数だけ確保することができる。従って、各データの記録期限を一定にすることができる。また、データ無効化装置は、前記一定の送信時間分のデータが常に一定のデータ量でない場合において、前記逐次無効化手段は前記無効化すべきと判断された部分データのうち前記新たな部分データを上書きするだけでは全て上書きできない部分に、さらに、任意のデータを上書きすることを特徴とすることもできる。

【0112】これによって、新たな部分データを上書きするだけでは全て上書きできない部分に、さらに、任意のデータを上書きすることができる。従って、無効化すべきデータを完全に破壊できる。また、データ無効化装置において、前記逐次無効化手段は前記新たな部分データの上書きを止めた後も先に記録されている部分データを全て無効化するまでは任意のデータを継続的に上書きすることを特徴とすることもできる。

【0113】これによって、新たな部分データの上書きを止めた後も任意のデータを継続的に上書きすることができる。従って、先に記録されている部分データを全て破壊することができる。また、データ無効化装置において、前記一の記録媒体には記録された各部分データの記録期限を管理するための期限管理情報が記録されており、前記判断手段は前記期限管理情報に基づいて記録期限が切れた部分データを無効化すべきと判断することを特徴とすることもできる。

【0114】これによって、記録期限が切れた部分データを無効化すべきと判断することができる。従って、各記録期限に基づいて各部分データを無効化するので、部分データ毎に優先度を持たせる等の設定が可能となり自由度が高くなる。また、前記データ無効化装置は、さらに、前記一の記録媒体に記録された対象データを前記部分データ単位で利用する利用手段を備え、前記判断手段は、さらに、前記利用手段により利用された部分データを無効化すべきと判断することを特徴とすることもできる。

【0115】これによって、さらに、利用された部分データも無効化すべきと判断することができる。従って、利用された部分データも無効化するので、複製品を許さないという趣旨をより逸脱せずにユーザの利便性を向上させることができる。また、前記データ無効化装置は、さらに、前記一の記録媒体に記録された対象データを前

10

20

30

40

50

記部分データ単位で利用する利用手段を備え、前記判断手段は前記利用手段により利用された部分データを無効化すべきと判断することを特徴とすることもできる。

【0116】これによって、利用された部分データを無効化すべきと判断することができる。従って、利用された部分データを無効化するので、再生されたり、コピーや移動された部分データを逐次無効化することにより、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができる。

【0117】また、データ無効化装置において、前記一の記録媒体に記録されている対象データは他の装置から送信されたコンテンツデータが記録されているものであり、前記送信されたコンテンツデータには前記対象データのコピーの可否を示すコピー制御情報が添付されており、前記利用手段は前記一の記録媒体に記録されたコンテンツデータを前記部分データ単位で再生するものであり、前記判断手段は前記送信されたコンテンツデータに添付されていたコピー制御情報がコピー不可を示していた場合に限り前記利用手段により再生された部分データに対応する前記一の記録媒体に記録された部分データを無効化すべきと判断をすることを特徴とすることもできる。

【0118】これによって、コピー制御情報がコピー不可を示していた場合に限り、部分データを無効化すべきと判断をすることができる。従って、コピー不可であるコンテンツデータに対してのみ、一時的にコピーする代わりにその複製品を無効化することできる。また、データ無効化装置において、前記一の記録媒体に記録されている対象データには前記対象データのコピーの可否を示すコピー制御情報が添付されており、前記利用手段は前記一の記録媒体に記録された対象データを前記部分データ単位でこの記録媒体に記録するものであり、前記判断手段は前記コピー制御情報がコピー不可を示している場合に限り前記利用手段により前記二の記録媒体に記録された部分データに対応する前記一の記録媒体に記録された部分データを無効化すべきと判断をすることを特徴とすることもできる。

【0119】これによって、コピー制御情報がコピー不可を示している場合に限り、部分データを無効化すべきと判断をすることができる。従って、コピー不可であるコンテンツデータに対してのみ、一時的にコピーする代わりにそのオリジナルを無効化することできる。また、データ無効化装置において、前記逐次無効化手段は、前記一の記録媒体上の前記判断手段により無効化すべきと判断された部分データを全て逐次破壊することを特徴とすることもできる。

【0120】これによって、無効化すべきと判断された部分データを全て逐次破壊することができる。従って、セキュリティを高めることができる。また、データ無効化装置において、前記逐次無効化手段は、前記一の記録

媒体上の前記判断手段により無効化すべきと判断された部分データのうちの部分データを利用する際に他のデータを利用するために先に必要となるデータを少なくとも逐次破壊することを特徴とすることもできる。

【0121】これによって、他のデータを利用するために先に必要となるデータを、少なくとも逐次破壊することができる。従って、装置の負荷の増大を最小限に抑えつつ、データを利用不能にすることができる。また、データ無効化装置において、前記一の記録媒体に記録されている対象データはIピクチャーを含むMPEGデータであり、前記先に必要となるデータはIピクチャーであることを特徴とすることもできる。

【0122】これによって、先に必要となるデータをMPEGデータ中のIピクチャーとすることができる。従って、BピクチャーやPピクチャーが残っていても参照すべきIピクチャーが破壊されていれば何の役にも立たず、Iピクチャー以外のBピクチャーやPピクチャー等を破壊しなければその分装置の負荷の増大を抑えることができる。

【0123】また、データ無効化装置において、前記一の記録媒体に記録されている対象データはIピクチャーを含むMPEGデータであり、前記先に必要となるデータはIピクチャーの先頭のセクタであることを特徴とすることもできる。これによって、先に必要となるデータをMPEGデータ中のIピクチャーの先頭のとすることができる。

【0124】従って、Iピクチャーを正常に再生できなくなり、さらにはBピクチャーやPピクチャーが残っていても参照すべきIピクチャーが正常に再生されなければ何の役にも立たず、残りの部分を破壊しなければその分装置の負荷の増大を抑えることができる。また、データ無効化装置において、前記逐次無効化手段は、自身の処理能力に余裕が無い場合には前記少なくとも逐次破壊する部分のデータのみを逐次破壊することを特徴とすることもできる。

【0125】これによって、自身の処理能力に余裕が無い場合には少なくとも逐次破壊する部分のデータのみを逐次破壊することができる。従って、装置の負荷の増大を抑えつつ、セキュリティも高めることができる。また、データ無効化装置において、前記逐次無効化手段は、自身の処理能力の余裕の範囲で前記少なくとも破壊する部分以外のデータを破壊することを特徴とすることもできる。

【0126】これによって、自身の処理能力の余裕の範囲で少なくとも破壊する部分以外のデータを破壊することができる。従って、装置の負荷の増大を抑えつつ、セキュリティも高めることができる。また、前記データ無効化装置は、さらに、前記無効化すべきと判断された部分データのうち前記逐次無効化手段により逐次破壊されなかった部分のデータを前記処理能力に余裕があ

る時に全て破壊する完全無効化手段を備えることを特徴とすることもできる。

【0127】逐次無効化手段により逐次破壊されなかった部分のデータを、処理能力に余裕がある時に全て破壊することができる。従って、装置の負荷の増大を抑えつつ、セキュリティも高めることができる。また、データ無効化装置において、前記一の記録媒体に記録されている対象データは前記部分データ毎に個別の部分データ暗号鍵を用いて暗号化されており、前記一の記録媒体には暗号化され記録された各部分データを復号するための各部分データ復号鍵が記録されており、前記逐次無効化手段は、前記一の記録媒体上の前記判断手段により無効化すべきと判断された部分データに対応する部分データ復号鍵を少なくとも逐次破壊することを特徴とすることもできる。

【0128】これによって、部分データ復号鍵を少なくとも逐次破壊することができるので、暗号化された各部分データが記録媒体上に残っていても復号することができないので役に立たない。従って、装置の負荷の増大を最小限に抑えつつ、データを利用不能にすることができる。

【0129】また、前記データ無効化装置は、さらに、暗号化された前記対象データを入手する入手手段と、入手手段により入手された暗号化された対象データを正当な使用者に予め配布された使用者鍵を用いて復号し対象データを生成する復号手段と、前記部分データ毎に任意の部分データ暗号鍵と対応する部分データ復号鍵とを生成する鍵生成手段と、復号手段により復号された対象データを前記部分データ毎に鍵生成手段により生成された部分データ暗号鍵を用いて対応する部分データ復号鍵によって復号可能に暗号化するデータ暗号化手段と、鍵生成手段により生成された部分データ復号鍵を当該データ無効化装置に固有の識別子を用いて暗号化する鍵暗号化手段と、データ暗号化手段により暗号化された部分データと対応する鍵暗号化手段により暗号化された部分データ復号鍵とを前記一の記録媒体に記録する記録手段とを備えることを特徴とすることもできる。

【0130】これによって、暗号化された対象データを使用者鍵を用いて復号し、部分データ毎に部分データ暗号鍵を用いて独自に暗号化し、また、部分データ復号鍵を装置に固有の識別子を用いて暗号化し、これらを記録媒体に記録することができる。従って、記録されたデータは、装置に固有の識別子を用いなければ復号できず、他の装置で利用することができないので、セキュリティを高めることができる。

【0131】また、前記データ無効化装置は、少なくとも、前記復号手段、前記鍵生成手段、前記データ暗号化手段、及び、鍵暗号化手段を同一の半導体チップ内に収めることを特徴とすることもできる。これによって、前記復号手段、前記鍵生成手段、前記データ暗号化手段、

及び、鍵暗号化手段が同一の半導体チップ内に収められるため、暗号化されていない状態の対象データが回路基盤の配線に出でこない。

【0132】従って、不正に対象データを得ようとする者が処理の途中から暗号化されていない状態の対象データを容易に取り出すことができないので、セキュリティを高めることができる。本発明に係るデータ無効化プログラムは、一の記録媒体に記録された対象データを無効化するデータ無効化プログラムであって、前記対象データは複数の部分データから構成され、コンピュータに、前記部分データ単位で前記一の記録媒体に記録された対象データを無効化すべきか否かを判断する判断ステップと、前記判断ステップにより所定数又は所定量の部分データに対して無効化すべきと判断される度に前記一の記録媒体に記録された対象データのうちの当該無効化すべきと判断された部分データを逐次無効化する逐次無効化ステップとを実行させることを特徴とする。

【0133】これによって、対象データを所定数又は所定量の部分データ毎に、所定の条件が満たされた部分データを逐次無効化することができる。従って、対象データの一時的な使用は許すが複製品の生成を禁止したり、1世代限りの複製品を許す等の場合において、禁止された複製品の生成を一時的に許す代わりにその複製品又はオリジナルを無効化することができ、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができる。

【0134】また、逐次複製品を無効化するので、悪意ある者が動作の途中で電源を抜くなどの小細工をして複製品を残そうとしても、所定数又は所定量の部分データの複製品を残す事が精一杯となるため、この単位を適切に選ぶことによりセキュリティを高めることができる。また、データ無効化プログラムにおいて、前記一の記録媒体は記録された各部分データの記録順序を示す順序情報を記録しており、前記判断ステップは前記順序情報により示される記録順序に基づいて先に記録された部分データから順番に無効化すべきと判断することを特徴とすることもできる。

【0135】これによって、先に記録された部分データから順番に無効化すべきと判断することができる。従って、先に記録された部分データから順番に無効化するので、常に新しい部分データだけを記録しておくことができる。また、データ無効化プログラムにおいて、前記一の記録媒体に記録されている対象データは他の装置から連続的に送信される送信データが現在の分まで継続的に記録されているものであり、前記データ無効化プログラムは、さらに、コンピュータに、前記送信データを受信する受信ステップを実行させ、前記逐次無効化ステップは、受信ステップにより受信された送信データを新たな部分データとし前記一の記録媒体内の前記判断ステップにより無効化すべきと判断された部分データが記録され

ている記録領域に前記新たな部分データを上書きすることにより当該新しい部分データを記録しつつ当該無効化すべきと判断された部分データを無効化することを特徴とすることもできる。

【0136】これによって、無効化すべきと判断された部分データが記録されている記録領域に、新たな部分データを上書きすることができる。従って、新しい部分データを記録することが無効化する処理を兼ねるので、無効化する処理が追加されたにもかかわらず装置の負荷がほとんど増加しない。また、データ無効化プログラムにおいて、前記一の記録媒体には記録された各部分データの記録期限を管理するための期限管理情報が記録されており、前記判断ステップは前記期限管理情報に基づいて記録期限が切れた部分データを無効化すべきと判断することを特徴とすることもできる。

【0137】これによって、記録期限が切れた部分データを無効化すべきと判断することができる。従って、各記録期限に基づいて各部分データを無効化するので、部分データ毎に優先度を持たせる等の設定が可能となり自由度が高くなる。また、前記データ無効化プログラムは、さらに、コンピュータに、前記一の記録媒体に記録された対象データを前記部分データ単位で利用する利用ステップを実行させ、前記判断ステップは、さらに、前記利用ステップにより利用された部分データを無効化すべきと判断することを特徴とすることもできる。

【0138】これによって、さらに、利用された部分データも無効化すべきと判断することができる。従って、利用された部分データも無効化するので、複製品を許さないという趣旨をより逸脱せずにユーザの利便性を向上させることができる。また、前記データ無効化プログラムは、さらに、コンピュータに、前記一の記録媒体に記録された対象データを前記部分データ単位で利用する利用ステップを実行させ、前記判断ステップは前記利用ステップにより利用された部分データを無効化すべきと判断することを特徴とすることもできる。

【0139】これによって、利用された部分データを無効化すべきと判断することができる。従って、利用された部分データを無効化するので、再生されたり、コピーや移動された部分データを逐次無効化することにより、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができる。

【0140】また、データ無効化プログラムにおいて、前記逐次無効化ステップは、前記一の記録媒体上の前記判断ステップにより無効化すべきと判断された部分データを全て逐次破壊することを特徴とすることもできる。これによって、無効化すべきと判断された部分データを全て逐次破壊することができる。

【0141】従って、セキュリティを高めることができる。また、データ無効化プログラムにおいて、前記逐次無効化ステップは、前記一の記録媒体上の前記判断手段

により無効化すべきと判断された部分データのうちの部分データを利用する際に他のデータを利用するために先に必要となるデータを少なくとも逐次破壊することを特徴とすることもできる。

【0142】これによって、他のデータを利用するために先に必要となるデータを、少なくとも逐次破壊することができる。従って、装置の負荷の増大を最小限に抑えつつ、データを利用不能にすることができる。また、データ無効化プログラムにおいて、前記一の記録媒体に記録されている対象データは前記部分データ毎に個別の部分データ暗号鍵を用いて暗号化されており、前記一の記録媒体には暗号化され記録された各部分データを復号するための各部分データ復号鍵が記録されており、前記逐次無効化ステップは、前記一の記録媒体上の前記判断手段により無効化すべきと判断された部分データに対応する部分データ復号鍵を少なくとも逐次破壊することを特徴とすることもできる。

【0143】これによって、部分データ復号鍵を少なくとも逐次破壊することができるので、暗号化された各部分データが記録媒体上に残っていても復号することができないので役に立たない。従って、装置の負荷の増大を最小限に抑えつつ、データを利用不能にすることができる。

【0144】本発明に係るデータ無効化方法は、一の記録媒体に記録された対象データを無効化するデータ無効化方法であって、前記対象データは複数の部分データから構成され、前記部分データ単位で前記一の記録媒体に記録された対象データを無効化すべきか否かを判断する判断ステップと、前記判断ステップにより所定数又は所定量の部分データに対して無効化すべきと判断される度に前記一の記録媒体に記録された対象データのうちの当該無効化すべきと判断された部分データを逐次無効化する逐次無効化ステップとを備えることを特徴とする。

【0145】これによって、対象データを所定数又は所定量の部分データ毎に、所定の条件が満たされた部分データを逐次無効化することができる。従って、対象データの一時的な使用は許すが複製品の生成を禁止したり、1世代限りの複製品を許す等の場合において、禁止された複製品の生成を一時的に許す代わりにその複製品又はオリジナルを無効化することができ、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができる。

【0146】また、逐次複製品を無効化するので、悪意ある者が動作の途中で電源を抜くなどの小細工をして複製品を残そうとしても、所定数又は所定量の部分データの複製品を残す事が精一杯となるため、この単位を適切に選ぶことによりセキュリティを高めることができる。また、データ無効化方法において、前記一の記録媒体は記録された各部分データの記録順序を示す順序情報を記録しており、前記判断ステップは前記順序情報によ

り示される記録順序に基づいて、先に記録された部分データから順番に無効化すべきと判断することを特徴とすることもできる。

【0147】これによって、先に記録された部分データから順番に無効化すべきと判断することができる。従って、先に記録された部分データから順番に無効化するので、常に新しい部分データだけを記録しておくことができる。また、データ無効化方法において、前記一の記録媒体に記録されている対象データは他の装置から連続的に送信される送信データが現在の分まで継続的に記録されているものであり、前記データ無効化方法は、さらに、前記送信データを受信する受信ステップを備え、前記逐次無効化ステップは、受信ステップにより受信された送信データを新たな部分データとし前記一の記録媒体内の前記判断ステップにより無効化すべきと判断された部分データが記録されている記録領域に前記新たな部分データを上書きすることにより当該新しい部分データを記録しつつ当該無効化すべきと判断された部分データを無効化することを特徴とすることもできる。

【0148】これによって、無効化すべきと判断された部分データが記録されている記録領域に、新たな部分データを上書きすることができる。従って、新しい部分データを記録することが無効化する処理を兼ねるので、無効化する処理が追加されたにもかかわらず装置の負荷がほとんど増加しない。また、データ無効化方法において、前記一の記録媒体には記録された各部分データの記録期限を管理するための期限管理情報が記録されており、前記判断ステップは前記期限管理情報に基づいて記録期限が切れた部分データを無効化すべきと判断することを特徴とすることもできる。

【0149】これによって、記録期限が切れた部分データを無効化すべきと判断することができる。従って、各記録期限に基づいて各部分データを無効化するので、部分データ毎に優先度を持たせる等の設定が可能となり自由度が高くなる。また、前記データ無効化方法は、さらに、前記一の記録媒体に記録された対象データを前記部分データ単位で利用する利用ステップを備え、前記判断ステップは、さらに、前記利用ステップにより利用された部分データを無効化すべきと判断することを特徴とすることもできる。

【0150】これによって、さらに、利用された部分データも無効化すべきと判断することができる。従って、利用された部分データも無効化するので、複製品を許さないという趣旨をより逸脱せずにユーザの利便性を向上させることができる。また、前記データ無効化方法は、さらに、前記一の記録媒体に記録された対象データを前記部分データ単位で利用する利用ステップを備え、前記判断ステップは前記利用ステップにより利用された部分データを無効化すべきと判断することを特徴とすることもできる。

【0151】これによって、利用された部分データを無効化すべきと判断することができる。従って、利用された部分データを無効化するので、再生されたり、コピーや移動された部分データを逐次無効化することにより、複製品を許さないという趣旨を逸脱せずにユーザの利便性を向上させることができる。

【0152】また、データ無効化方法において、前記逐次無効化ステップは、前記一の記録媒体上の前記判断ステップにより無効化すべきと判断された部分データを全て逐次破壊することを特徴とすることもできる。これによって、無効化すべきと判断された部分データを全て逐次破壊することができる。

【0153】従って、セキュリティを高めることができる。また、データ無効化方法において、前記逐次無効化ステップは、前記一の記録媒体上の前記判断手段により無効化すべきと判断された部分データのうちの部分データを利用する際に他のデータを利用するために先に必要となるデータを少なくとも逐次破壊することを特徴とすることもできる。

【0154】これによって、他のデータを利用するために先に必要となるデータを、少なくとも逐次破壊することができる。従って、装置の負荷の増大を最小限に抑えつつ、データを利用不能にすることができる。また、データ無効化方法において、前記一の記録媒体に記録されている対象データは前記部分データ毎に個別の部分データ暗号鍵を用いて暗号化されており、前記一の記録媒体には暗号化され記録された各部分データを復号するための各部分データ復号鍵が記録されており、前記逐次無効化ステップは、前記一の記録媒体上の前記判断手段により無効化すべきと判断された部分データに対応する部分データ復号鍵を少なくとも逐次破壊することを特徴とすることもできる。

【0155】これによって、部分データ復号鍵を少なくとも逐次破壊することができるので、暗号化された各部分データが記録媒体上に残っていても復号することができないので役に立たない。従って、装置の負荷の増大を最小限に抑えつつ、データを利用不能にすることができる。

【図面の簡単な説明】

【図1】本発明の実施の形態1に係る受信再生無効化装置のハードウェア構成の一例を示す図である。

【図2】本発明の実施の形態1に係る受信再生無効化装置の機能ブロック図である。

【図3】本発明の実施の形態1に係る受信再生無効化装置の動作の一例を示す図である。

【図4】本発明の実施の形態1に係る受信再生無効化装置の動作の別の例を示す図である。

【図5】本発明の実施の形態2に係る受信再生無効化装置の機能ブロック図である。

【図6】本発明の実施の形態2に係る受信再生無効化装

置の動作の一例を示す図である。

【図7】本発明の実施の形態3に係る受信再生無効化装置の機能ブロック図である。

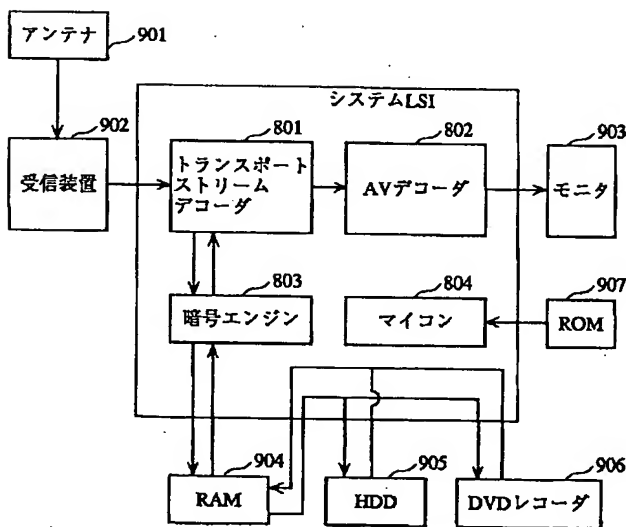
【図8】本発明の実施の形態3に係る受信再生無効化装置の動作の一例を示す図である。

【符号の説明】

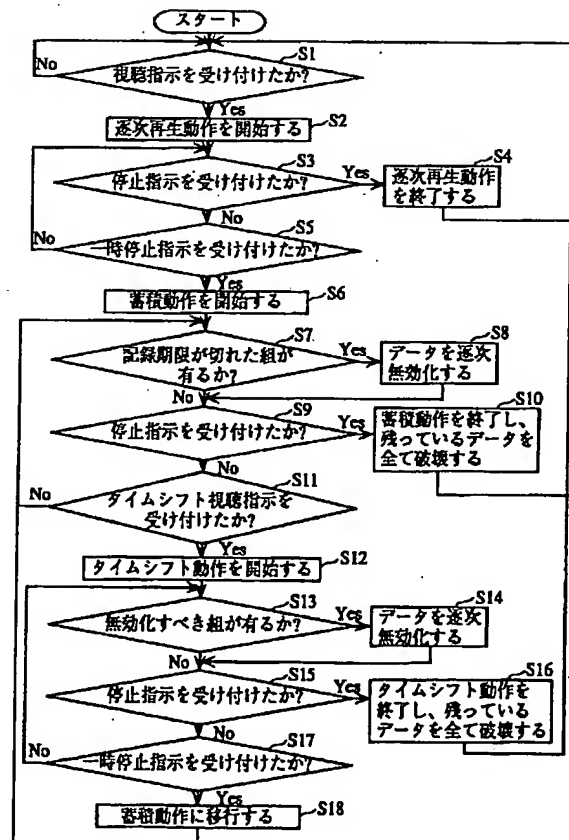
- 100 受信再生無効化装置
- 101 ユーザインタフェース部
- 102 受信部
- 103 デスクランブル部
- 104 個別鍵生成部
- 105 データ暗号化部
- 106 鍵暗号化部
- 107 記録部
- 108 鍵復号部
- 109 データ復号部
- 110 再生部

- * 111 無効化判断部
- 112 処理能力判断部
- 113 逐次無効化部
- 114 完全無効化部
- 200 受信再生無効化装置
- 201 記録部
- 202 無効化判断部
- 203 逐次無効化部
- 204 完全無効化部
- 10 300 受信再生無効化装置
- 301 移動部
- 302 無効化判断部
- 800 システムLSI
- 801 トランスポートストリームデコーダ
- 802 AVデコーダ
- 803 暗号エンジン
- * 804 マイコン

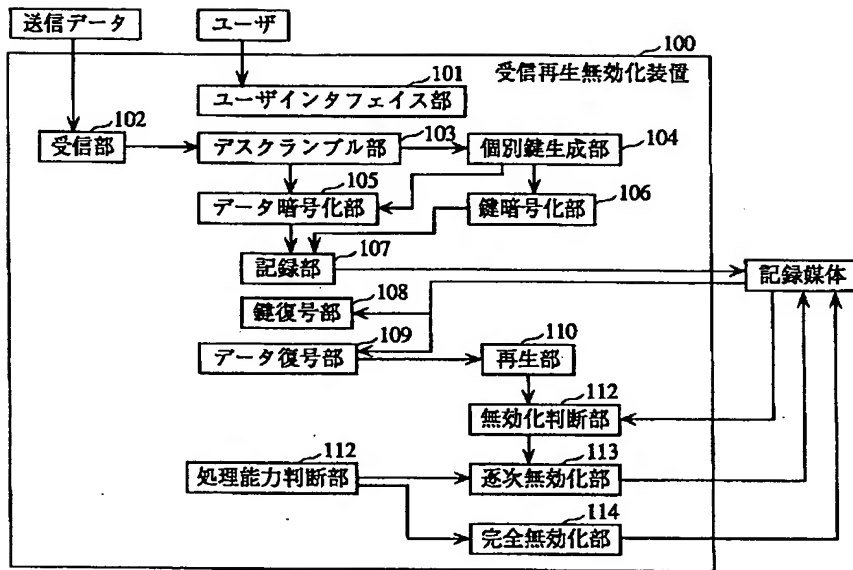
【図1】



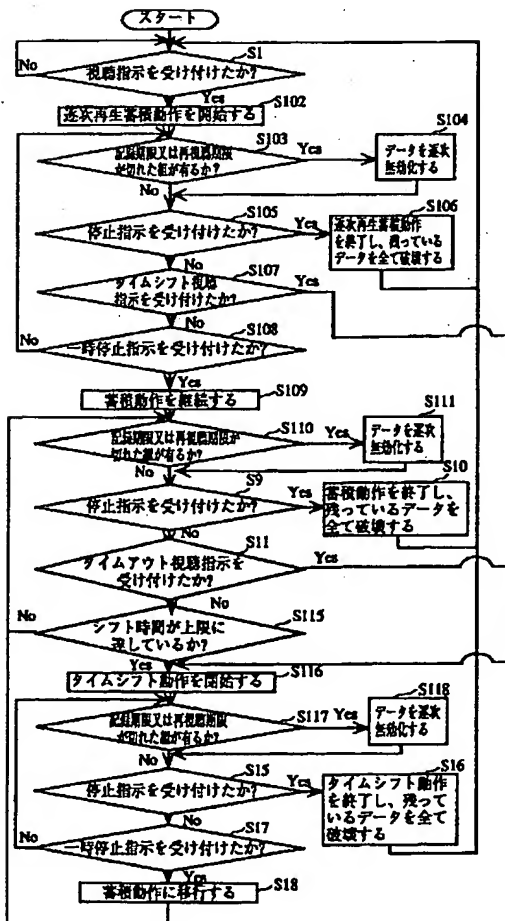
【図3】



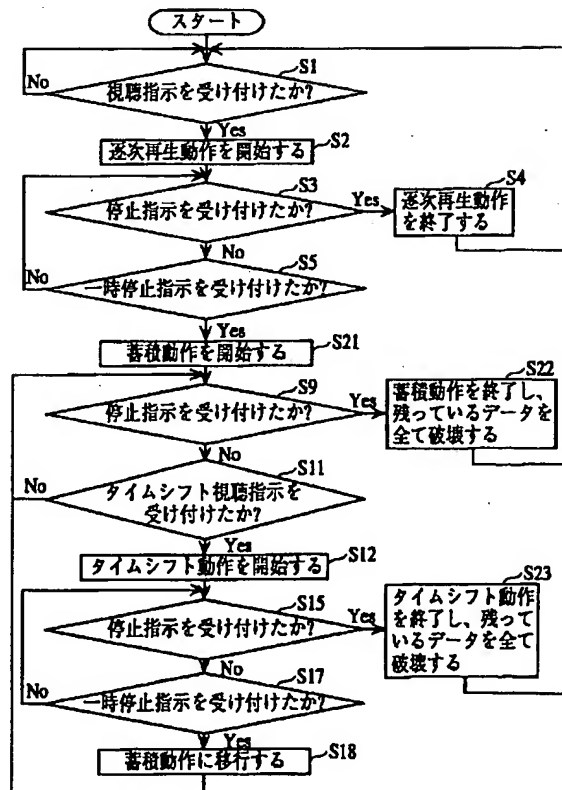
【図2】



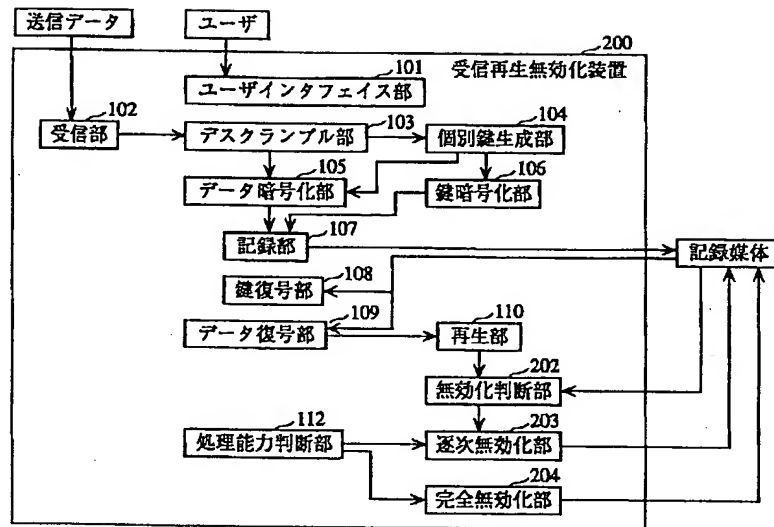
【図4】



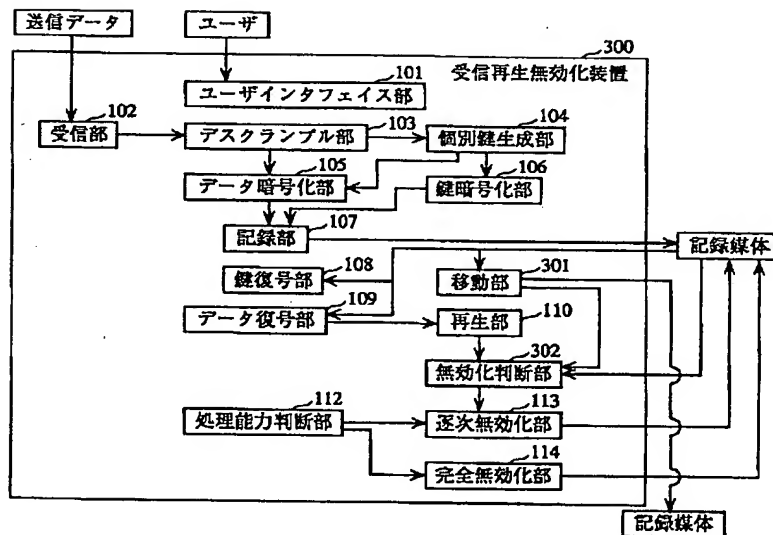
【図6】



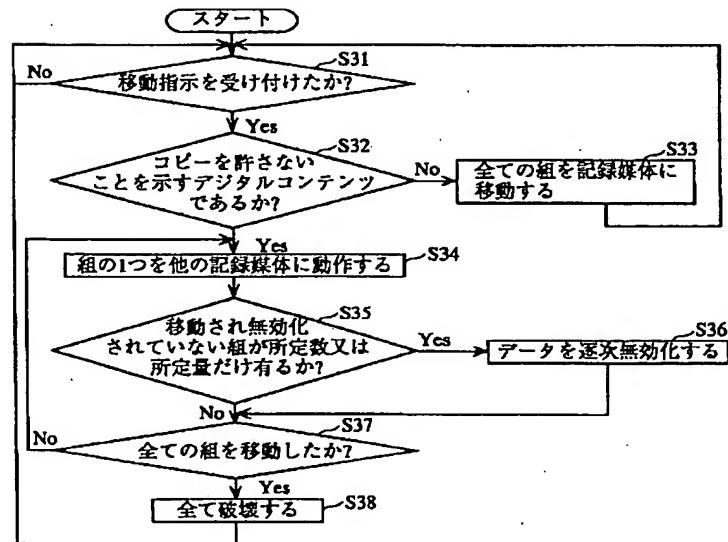
【図5】



【図7】



【図8】



フロントページの続き

(51) Int. Cl. ⁷

H 0 4 N 5/781
5/85
5/91

識別記号

F I

H 0 4 N 5/781
5/91.

テーマコード (参考)

5 1 0 F
P

(72) 発明者 宮▲ざき▼ 雅也

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

F ターム (参考) 5B017 AA07 BA07 BA08 BB10 CA16
5C052 AA02 AB03 AB04 CC06 DD10
5C053 FA13 FA23 FA24 GB06 JA21
KA24 LA07
5J104 NA02 PA14

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第6部門第3区分

【発行日】平成20年2月7日(2008.2.7)

【公開番号】特開2002-244926(P2002-244926A)

【公開日】平成14年8月30日(2002.8.30)

【出願番号】特願2001-39140(P2001-39140)

【国際特許分類】

G 0 6 F 12/14 (2006.01)

G 0 6 Q 50/00 (2006.01)

H 0 4 N 5/85 (2006.01)

H 0 4 L 9/08 (2006.01)

H 0 4 N 5/765 (2006.01)

H 0 4 N 5/781 (2006.01)

H 0 4 N 5/91 (2006.01)

【F I】

G 0 6 F 12/14 3 2 0 D

G 0 6 F 12/14 3 2 0 E

G 0 6 F 17/60 1 4 2

H 0 4 N 5/85 Z

H 0 4 L 9/00 6 0 1 C

H 0 4 N 5/781 5 1 0 F

H 0 4 N 5/91 P

【手続補正書】

【提出日】平成19年12月14日(2007.12.14)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

一の記録媒体に記録された対象データを無効化するデータ無効化装置であって、前記対象データは、複数の部分データから構成され、前記部分データ単位で前記一の記録媒体に記録された対象データを、無効化すべきか否かを判断する判断手段と、前記判断手段により所定数又は所定量の部分データに対して無効化すべきと判断される度に、前記一の記録媒体に記録された対象データのうちの、当該無効化すべきと判断された部分データを逐次無効化する逐次無効化手段とを備えることを特徴とするデータ無効化装置。

【請求項2】

前記一の記録媒体は、記録された各部分データの記録順序を示す順序情報を記録しており、前記判断手段は、前記順序情報により示される記録順序に基づいて、先に記録された部分データから順番に無効化すべきと判断することを特徴とする請求項1に記載のデータ無効化装置。

【請求項3】

前記一の記録媒体に記録されている対象データは、他の装置から連続的に送信される送信データが、現在の分まで継続的に記録されているものであり、前記データ無効化装置は、さらに、前記送信データを受信する受信手段を備え、前記逐次無効化手段は、受信手段により受信された送信データを新たな部分データとし、前記一の記録媒体内の前記判断手段により無効化すべきと判断された部分データが記録されている記録領域に、前記新たな

部分データを上書きすることにより、当該新しい部分データを記録しつつ当該無効化すべきと判断された部分データを無効化することを特徴とする請求項 2 に記載のデータ無効化装置。

【請求項 4】

前記部分データはそれぞれ、前記送信データの一定の送信時間分のデータであり、前記一の記録媒体には、前記一定の送信時間分のデータを記録するための記録領域が規定数だけ確保されることを特徴とする請求項 3 に記載のデータ無効化装置。

【請求項 5】

前記一定の送信時間分のデータが、常に一定のデータ量でない場合において、前記逐次無効化手段は、前記無効化すべきと判断された部分データのうち、前記新たな部分データを上書きするだけでは全て上書きできない部分に、さらに、任意のデータを上書きすることを特徴とする請求項 4 に記載のデータ無効化装置。

【請求項 6】

前記逐次無効化手段は、前記新たな部分データの上書きを止めた後も、先に記録されている部分データを全て無効化するまでは、任意のデータを継続的に上書きすることを特徴とする請求項 4 及び 5 の何れか 1 項に記載のデータ無効化装置。

【請求項 7】

前記一の記録媒体には、記録された各部分データの記録期限を管理するための期限管理情報が記録されており、前記判断手段は、前記期限管理情報に基づいて、記録期限が切れた部分データを無効化すべきと判断することを特徴とする請求項 1 に記載のデータ無効化装置。

【請求項 8】

前記データ無効化装置は、さらに、前記一の記録媒体に記録された対象データを、前記部分データ単位で利用する利用手段を備え、前記判断手段は、さらに、前記利用手段により利用された部分データを無効化すべきと判断することを特徴とする請求項 2 及び 7 の何れか 1 項に記載のデータ無効化装置。

【請求項 9】

前記データ無効化装置は、さらに、前記一の記録媒体に記録された対象データを、前記部分データ単位で利用する利用手段を備え、前記判断手段は、前記利用手段により利用された部分データを無効化すべきと判断することを特徴とする請求項 1 に記載のデータ無効化装置。

【請求項 10】

前記一の記録媒体に記録されている対象データは、他の装置から送信されたコンテンツデータが記録されているものであり、前記送信されたコンテンツデータには、前記対象データのコピーの可否を示すコピー制御情報が添付されており、前記利用手段は、前記一の記録媒体に記録されたコンテンツデータを、前記部分データ単位で再生するものであり、前記判断手段は、前記送信されたコンテンツデータに添付されていたコピー制御情報がコピー不可を示していた場合に限り、前記利用手段により再生された部分データに対応する、前記一の記録媒体に記録された部分データを無効化すべきと判断することを特徴とする請求項 8 及び 9 の何れか 1 項に記載のデータ無効化装置。

【請求項 11】

前記一の記録媒体に記録されている対象データには、前記対象データのコピーの可否を示すコピー制御情報が添付されており、前記利用手段は、前記一の記録媒体に記録された対象データを、前記部分データ単位で、二の記録媒体に記録するものであり、前記判断手段は、前記コピー制御情報がコピー不可を示している場合に限り、前記利用手段により前記二の記録媒体に記録された部分データに対応する、前記一の記録媒体に記録された部分データを無効化すべきと判断することを特徴とする請求項 9 に記載のデータ無効化装置。

【請求項 12】

前記逐次無効化手段は、前記一の記録媒体上の、前記判断手段により無効化すべきと判

断された部分データを全て逐次破壊することを特徴とする請求項1～11の何れか1項に記載のデータ無効化装置。

【請求項13】

前記逐次無効化手段は、前記一の記録媒体上の、前記判断手段により無効化すべきと判断された部分データのうちの、部分データを利用する際に、他のデータを利用するために先に必要となるデータを、少なくとも逐次破壊することを特徴とする請求項1、2及び7～11の何れか1項に記載のデータ無効化装置。

【請求項14】

前記一の記録媒体に記録されている対象データは、Iピクチャーを含むMPEGデータであり、前記先に必要となるデータは、Iピクチャーであることを特徴とする請求項13に記載のデータ無効化装置。

【請求項15】

前記一の記録媒体に記録されている対象データは、Iピクチャーを含むMPEGデータであり、前記先に必要となるデータは、Iピクチャーの先頭のセクタであることを特徴とする請求項13に記載のデータ無効化装置。

【請求項16】

前記逐次無効化手段は、自身の処理能力に余裕が無い場合には、前記少なくとも逐次破壊するとした部分のデータのみを逐次破壊することを特徴とする請求項13～15の何れか1項に記載のデータ無効化装置。

【請求項17】

前記逐次無効化手段は、自身の処理能力の余裕の範囲で、前記少なくとも破壊するとした部分以外のデータを破壊することを特徴とする請求項16に記載のデータ無効化装置。

【請求項18】

前記データ無効化装置は、さらに、前記無効化すべきと判断された部分データのうちの、前記逐次無効化手段により逐次破壊されなかった部分のデータを、前記処理能力に余裕がある時に全て破壊する完全無効化手段を備えることを特徴とする請求項16及び17の何れか1項に記載のデータ無効化装置。

【請求項19】

前記一の記録媒体に記録されている対象データは、前記部分データ毎に個別の部分データ暗号鍵を用いて暗号化されており、前記一の記録媒体には、暗号化され記録された各部分データを復号するための各部分データ復号鍵が記録されており、前記逐次無効化手段は、前記一の記録媒体上の、前記判断手段により無効化すべきと判断された部分データに対応する部分データ復号鍵を、少なくとも逐次破壊することを特徴とする請求項1、2及び7～11の何れか1項に記載のデータ無効化装置。

【請求項20】

前記データ無効化装置は、さらに、暗号化された前記対象データを入手する入手手段と、入手手段により入手された暗号化された対象データを、正当な使用者に予め配布された使用者鍵を用いて復号し、対象データを生成する復号手段と、前記部分データ毎に、任意の部分データ暗号鍵と、対応する部分データ復号鍵とを生成する鍵生成手段と、復号手段により復号された対象データを、前記部分データ毎に、鍵生成手段により生成された部分データ暗号鍵を用いて、対応する部分データ復号鍵によって復号可能に暗号化するデータ暗号化手段と、鍵生成手段により生成された部分データ復号鍵を、当該データ無効化装置に固有の識別子を用いて暗号化する鍵暗号化手段と、データ暗号化手段により暗号化された部分データと、対応する鍵暗号化手段により暗号化された部分データ復号鍵とを、前記一の記録媒体に記録する記録手段とを備えることを特徴とする請求項19に記載のデータ無効化装置。

【請求項21】

前記データ無効化装置は、少なくとも、前記復号手段、前記鍵生成手段、前記データ暗号化手段、及び、鍵暗号化手段を、同一の半導体チップ内に収めることを特徴とする請求項20に記載のデータ無効化装置。

【請求項 2 2】

一の記録媒体に記録された対象データを無効化するデータ無効化プログラムであって、前記対象データは、複数の部分データから構成され、コンピュータに、前記部分データ単位で前記一の記録媒体に記録された対象データを、無効化すべきか否か判断する判断ステップと、前記判断ステップにより所定数又は所定量の部分データに対して無効化すべきと判断される度に、前記一の記録媒体に記録された対象データのうちの、当該無効化すべきと判断された部分データを逐次無効化する逐次無効化ステップとを実行させることを特徴とするデータ無効化プログラム。

【請求項 2 3】

一の記録媒体に記録された対象データを無効化するデータ無効化方法であって、前記対象データは、複数の部分データから構成され、前記部分データ単位で前記一の記録媒体に記録された対象データを、無効化すべきか否か判断する判断ステップと、前記判断ステップにより所定数又は所定量の部分データに対して無効化すべきと判断される度に、前記一の記録媒体に記録された対象データのうちの、当該無効化すべきと判断された部分データを逐次無効化する逐次無効化ステップとを備えることを特徴とするデータ無効化方法。